Annals of Pure and Applied Logic 46 (1990) 1–40
North-Holland

DIOPHANTINE INDUCTION

Richard KAYE
Jesus College, Oxford OX1 3DW, England, UK

Communicated by D. van Dalen
Received 29 July 1988

We show that Matijasevič's Theorem on the diophantine representation of r.e. predicates is provable in the subsystem $I\exists_1^-$ of Peano Arithmetic formed by restricting the induction scheme to diophantine formulas with no parameters. More specifically,

$$I\exists_1^- \vdash IE_1^- + E \vdash \text{Matijasevič's Theorem}$$

where IE_1^- is the scheme of parameter-free bounded existential induction and E is an $\forall\exists$ axiom expressing the existence of a function of exponential growth. (We prove this by means of a conservation result relating parameter and parameter-free induction schemes which is of independent interest.) We conclude by examining the consequences of these results to the structure of countable nonstandard models of IE_1^-.

1. Introduction

Fix $\mathscr{L} = \{0, 1, +, \cdot, <\}$, the usual language of arithmetic, and $\mathbb{N}$ the standard model for $\mathscr{L}$, i.e. the model with domain consisting of the set of nonnegative integers where 0, 1, +, ·, < have the obvious interpretation. We write $\exists x\,(x < t \to \cdots)$ and $\exists x\,(x < t \wedge \cdots)$ as $\forall x < t \cdots$ and $\exists x < t \cdots$ as usual, and call these quantifiers *bounded*. We define the formula classes E_n, U_n, $\exists_n$, $\forall_n$, Δ_0, Σ_n, Π_n in the usual way as follows:

$$E_0 = U_0 = \exists_0 = \forall_0 = \{\phi(\boldsymbol{x}) \in \mathscr{L} \mid \phi \text{ is quantifier free}\},$$
$$\exists_{n+1} = \{\exists \boldsymbol{y}\, \phi(\boldsymbol{x}, \boldsymbol{y}) \mid \phi \in \forall_n\},$$
$$\forall_{n+1} = \{\forall \boldsymbol{y}\, \phi(\boldsymbol{x}, \boldsymbol{y}) \mid \phi \in \exists_n\},$$
$$E_{n+1} = \{\exists \boldsymbol{y} < t(\boldsymbol{x})\, \phi(\boldsymbol{x}, \boldsymbol{y}) \mid \phi \in U_n,\ t \text{ a term of } \mathscr{L}\},$$
$$U_{n+1} = \{\forall \boldsymbol{y} < t(\boldsymbol{x})\, \phi(\boldsymbol{x}, \boldsymbol{y}) \mid \phi \in E_n,\ t \text{ a term of } \mathscr{L}\},$$
$$\Delta_0 = \Sigma_0 = \Pi_0 = \bigcup_{n\in\mathbb{N}} E_n = \bigcup_{n\in\mathbb{N}} U_n,$$
$$\Sigma_{n+1} = \{\exists \boldsymbol{y}\, \phi(\boldsymbol{x}, \boldsymbol{y}) \mid \phi \in \Pi_n\},$$
$$\Pi_{n+1} = \{\forall \boldsymbol{y}\, \phi(\boldsymbol{x}, \boldsymbol{y}) \mid \phi \in \Sigma_n\}.$$

If $\mathscr{L}'$ is a language extending $\mathscr{L}$ we define the corresponding formula classes, $E_n(\mathscr{L}')$, $U_n(\mathscr{L}')$ etc. of $\mathscr{L}'$ in the same way.

PA^- denotes a finite set of $\forall E_1$ axioms (i.e. each axiom is the universal closure of an E_1 formula) in $\mathscr{L}$ whose models are exactly the nonnegative parts of

discretely ordered rings. For a class Γ of formulas, $I\Gamma$ denotes PA^- together with the *induction scheme*

$$\forall \boldsymbol{a}\,((\theta(0, \boldsymbol{a}) \wedge \forall x\,(\theta(x, \boldsymbol{a}) \rightarrow \theta(x+1, \boldsymbol{a}))) \rightarrow \forall x\,\theta(x, \boldsymbol{a}))$$

for each formula $\theta(x, \boldsymbol{a}) \in \Gamma$. The variables $\boldsymbol{a}$ are called *parameters* and x is the *induction variable*. IE_0 (which is the same as IU_0, $I\exists_0$ and $I\forall_0$) will be denoted *IOpen*, and is the theory studied by Shepherdson in [10].

The theory $L\Gamma$ is PA^- together with the *least number principle*,

$$\forall \boldsymbol{a}\,(\exists x\,\theta(x, \boldsymbol{a}) \rightarrow \exists y\,(\theta(y, \boldsymbol{a}) \wedge \forall x < y\, \neg\theta(x, \boldsymbol{a})))$$

for all $\theta(x, \boldsymbol{a}) \in \Gamma$. We recall the

Result 1.1. (i) (Paris–Kirby, [7]) *For all* $n \in \mathbb{N}$

$$I\Sigma_n \dashv\vdash I\Pi_n \dashv\vdash L\Sigma_n \dashv\vdash L\Pi_n.$$

(ii) (Wilmers, [12]) *For all* $n \geqslant 1$

$$IE_n \dashv\vdash IU_n \dashv\vdash LE_n.$$

(iii) (By the same argument as in [12]) *For all* $n \geqslant 1$

$$I\exists_n \dashv\vdash I\forall_n \dashv\vdash L\exists_n.$$

Remark. This result holds equally well for theories $I\Sigma_n(\mathscr{L}')$, etc. for some $\mathscr{L}' \supset \mathscr{L}$.

We shall also consider the theories of *parameter-free* induction, $I\Gamma^-$, which is PA^- together with,

$$(\theta(0) \wedge \forall x\,(\theta(x) \rightarrow \theta(x+1))) \rightarrow \forall x\,\theta(x)$$

for each $\theta(x) \in \Gamma$ with only one free variable.

In [3] it is shown that there is a Δ_0 formula $\eta(x, y, z)$ that represents the graph of exponentiation with most of the usual properties provable in $I\Delta_0$. In particular,

$$I\Delta_0 \vdash \forall x\,\eta(x, 0, 1) \wedge \forall y > 0\,\eta(0, y, 0),$$

$$I\Delta_0 \vdash \forall x, y, z, w\,(\eta(x, y, z) \wedge \eta(x, y, w) \rightarrow z = w),$$

$$I\Delta_0 \vdash \forall x, y, z\,(\eta(x, y, z) \rightarrow \eta(x, y+1, xz).$$

The sentence exp which is,

$$\forall x, y\,\exists z\,\eta(x, y, z)$$

is however not provable in $I\Delta_0$. (In the sequel we will often denote $\eta(x, y, z)$ by the more suggestive $x^y = z$.)

Dimitracopoulos and Gaifman go on to show that Matijasevič's Theorem on the diophantine representation of r.e. sets is provable in the theory $I\Delta_0 + \exp$.

More specifically they show,

Result 1.2. *for all* $\theta \in \Sigma_1$ *there is* $\psi \in \exists_1$ *such that,*

$$I\Delta_0 + \exp \vdash \forall \boldsymbol{x}\, (\theta(\boldsymbol{x}) \leftrightarrow \psi(\boldsymbol{x}))$$

This raises the obvious question: can either '$I\Delta_0$' or 'exp' be significantly reduced here? Since Matijasevič's Theorem is 'about' diophantine (or equivalently $\exists_1$, see 1.4 below) formulas another intriguing and related question (posed by Z. Adamowicz) is: does $I\exists_1$ prove Matijasevič's Theorem?

The problem '$I\Delta_0 \vdash$ Matijasevič's Theorem?' is still unsolved, but by replacing exp by a more suitable $\forall\exists$ axiom, denoted E, we are able to show that,

$$IE_1 + E \vdash \text{Matijasevič's Theorem}$$

and indeed $IE_1 + E$ and $I\Delta_0 + \exp$ are equivalent. Since $I\exists_1 \vdash IE_1 + E$ we obtain a positive answer to Adamowicz's question. The methods we use are taken from the work of Robinson, Davis and Putnam but formalized in the appropriate theory. It turns out that by making heavy use of parameters in our induction schemes we are able to prove a rudimentary version of Matijasevič's Theorem which is nevertheless strong enough to deduce $IE_1 + E \dashv\vdash I\Delta_0 + \exp$. The full Matijasevič's Theorem in $IE_1 + E$ then follows by Dimitracopoulos and Gaifman's work.

The main idea behind our proof of Matijasevič's Theorem in $IE_1 + E$ is as follows. Considering an arbitrary nonstandard model M of $IE_1 + E$ and an element $a \in M$, we can find, for each Δ_0 formula $\theta(x)$, an E_1 formula $\psi_\theta(x)$ which is equivalent to $\theta(x)$ for all x in M less than a. This formula $\psi_\theta(x)$ is obtained by consideration of the work of Robinson, Davis and Putnam on Hilbert's 10th Problem: $\psi_\theta(x)$ will, typically, contain extra parameters $\boldsymbol{b}$, and the use of these parameters allows us to bypass the most difficult part of the solution to Hilbert's 10th problem by replacing the usual diophantine function of exponential growth with a very much simpler one. The existence of the $\psi_\theta(x)$ together with IE_1 in M is, however, sufficient to show that M satisfies Δ_0 induction up to a, and so (since a is arbitrary) $M \vDash I\Delta_0$. It then follows from the axiom E that $M \vDash I\Delta_0 + \exp$, and hence, by Dimitracopoulos and Gaifman's work, M satisfies the full Matijasevič Theorem.

Clearly the conception of this outline argument is model-theoretic, and we feel it is most natural to adhere to model-theoretic notation, especially as we can utilize various devices that allow us to suppress the mention of the parameters, thus simplifying our notation considerably (see Theorems 2.7 and 3.4). It would be quite straightforward (albeit rather tedious) to use the details we give to obtain a direct proof.

In Section 5 we shift our attention to parameter-free induction. Our goal is to show $I\exists_1^- \vdash$ Matijasevič's Theorem and $IE_1^- + E \dashv\vdash I\Delta_0 + \exp$. The key result

needed to prove these facts is the conservation result,

If $\sigma \in \exists_{n+2}$ *is a sentence and* $I\exists_n \vdash \sigma$ *then* $I\exists_n^- \vdash \sigma$, and
If $\sigma \in \exists\forall E_n$ *is a sentence and* $IE_n \vdash \sigma$ *then* $IE_n^- \vdash \sigma$.

(Analogous results for the theories $I\Sigma_n^-$ and $B\Sigma_n^-$ are presented in [4].)

To apply this we need an additional result on axiomatizations of theories that prove Matijasevič's Theorem. It has been known for some time that $I\Delta_0 + \exp$ is $\forall_2$ axiomatizable, a result first proved by Handley and Paris (unpublished), but the situation is in fact more general than this: we present a new and very simple proof that any Π_n theory (for $n \geqslant 2$) that proves Matijasevič's Theorem has an $\forall_n$ axiomatization.

It now follows easily that $I\exists_1^- \vdash I\Delta_0 + \exp$ and hence $I\exists_1^-$ proves Matijasevič's Theorem. In fact, by using a result somewhat akin to Parikh's Theorem (Result 1.3 below) we will also be able to deduce that $IE_1^- + E \vdash I\Delta_0 + \exp$. We should mention however that, although the direct proofs of Matijasevič's Theorem in $I\exists_1$ and $IE_1 + E$ could be obtained rather easily, the conservation results above do not preserve lengths of proofs (this is because, in their proof-theoretic analysis, these results depend heavily on cut-elimination) and so the analogous proofs in $I\exists_1^-$ and $IE_1^- + E$ are very much longer. We will say more about this later.

Interest in $I\exists_1^-$ and IE_1^- was initially generated by the conjecture that these theories fail to satisfy Tennenbaum's Theorem, that is they may have recursive nonstandard models. Recursive nonstandard models for *IOpen* [10] and $I\forall_1^-$ [13] have been exhibited, whereas it is known that no such models exist for IE_1 or $I\exists_1$ [12]. $I\exists_1^-$ and IE_1^- were therefore considered natural candidates for theories sufficiently weak to have recursive models. In fact we can now show that this is not the case for $I\exists_1^-$ using Matijasevič's Theorem. It follows from our work here that $I\exists_1^- \dashv\vdash I\Sigma_1^-$ and it is well known that $I\Sigma_1^- \vdash I\Delta_0^- \dashv\vdash I\Delta_0$. (This is a corollary of our conservation result for IE_n^-. A direct proof appears in [4].) Hence $I\exists_1^- \vdash IE_1$ so by work in [12] cannot have recursive models. In Section 6 we examine this question for IE_1^-.

The work presented here forms part of the author's Ph.D. thesis at Manchester University. I would like to take this opportunity to thank Jeff Paris and George Wilmers for encouragement and many helpful remarks on this work, and everyone at Manchester for making my three years there such happy ones.

The rest of this introduction is devoted to presenting background material that will be necessary later.

A formula $\psi(\boldsymbol{x})$ *is* ∇_1 (in a language $\mathscr{L}'$) iff it is equivalent to both an $E_1(\mathscr{L}')$ formula $\theta(\boldsymbol{x})$ and a $U_1(\mathscr{L}')$ formula $\phi(\boldsymbol{x})$. $\psi(\boldsymbol{x})$ is ∇_1 *in a theory* T iff T proves the equivalence $\forall \boldsymbol{x}\,(\theta(\boldsymbol{x}) \leftrightarrow \psi(\boldsymbol{x}) \leftrightarrow \phi(\boldsymbol{x}))$. A function f is E_1 iff it is represented by

an E_1 formula $\theta(\boldsymbol{x}, y)$ with

$$\forall \boldsymbol{x}\, \exists! y\, \theta(\boldsymbol{x}, y) \wedge \forall \boldsymbol{x}\, \theta(\boldsymbol{x}, f(\boldsymbol{x})).$$

$f(\boldsymbol{x})$ is E_1 *in a theory* T iff T proves the sentence $\forall \boldsymbol{x}\, \exists! y\, \theta(\boldsymbol{x}, y)$.

For example the function $\lfloor x/y \rfloor$ = integer part of x/y (if $y > 0$) or 0 (if $y = 0$) is E_1 in *IOpen*. It is represented by

$$\lfloor x/y \rfloor = z \overset{\text{def}}{\longleftrightarrow} (y = 0 \wedge z = 0) \vee (y > 0 \wedge yz \leqslant x < y(z+1))$$

and supposing there is no z such that $z = \lfloor a/b \rfloor$ in a model of *IOpen*, by considering induction on the formula $ax \leqslant b$ we obtain a contradiction, hence

$$IOpen \vdash \forall x, y\, \exists! z\, \lfloor x/y \rfloor = z.$$

The relation $a \mid b$, which is defined as,

$$\exists c \leqslant b\, (ac = b)$$

is ∇_1 in *IOpen*, as it is equivalent to

$$\forall c \leqslant b\, (c = \lfloor b/a \rfloor \rightarrow ac = b).$$

The importance of ∇_1 relations and E_1 functions is that we may ignore them when computing the quantifier complexity of formulas involving them. For example if ϕ (not quantifier free) involves $\lfloor x/y \rfloor$ we may replace any subformula $\theta(\boldsymbol{x}, \lfloor x/y \rfloor)$ of ϕ by either

$$\exists z \leqslant x\, (z = \lfloor x/y \rfloor \wedge \theta(\boldsymbol{x}, z))$$

or

$$\forall z \leqslant x\, (z = \lfloor x/y \rfloor \rightarrow \theta(\boldsymbol{x}, z))$$

to obtain a formula of the required complexity equivalence to ϕ. Similarly if ϕ contains a ∇_1 relation $R(\boldsymbol{x})$ we can replace all occurrences of R by either the E_1 form or the U_1 form, to reduce ϕ to a formula in the original language of the same quantifier complexity. If ϕ contains a function $f(\boldsymbol{x})$ which is E_1 in the theory T, we may replace $\theta(\boldsymbol{x}, f(\boldsymbol{x}))$ by $\exists z \leqslant t(\boldsymbol{x})(z = f(\boldsymbol{x}) \wedge \theta(\boldsymbol{x}, z))$ or $\forall z \leqslant t(\boldsymbol{x})(z = f(\boldsymbol{x}) \rightarrow \theta(\boldsymbol{x}, z))$ provided a term $t(\boldsymbol{x})$ can be found that bounds f. That this can always be done if f is a E_1 function in a Π_1 theory is shown by the following result:

Result 1.3 (Parikh). *If $T \vdash PA^-$ is a Π_1 theory in a language $\mathscr{L}' \supseteq \mathscr{L}$ such that for every term $t(\boldsymbol{x})$ of $\mathscr{L}'$ there is a term $\sigma_t(\boldsymbol{x})$ of $\mathscr{L}'$ with $T \vdash \forall \boldsymbol{x}, \boldsymbol{y}\, (\bigwedge_i x_i \leqslant y_i \rightarrow t(\boldsymbol{x}) \leqslant \sigma_t(\boldsymbol{y}))$ and if $T \vdash \forall \boldsymbol{x}\, \exists \boldsymbol{y}\, \theta(\boldsymbol{x}, \boldsymbol{y})$ with θ a Δ_0 formula of $\mathscr{L}'$, there is a term s of $\mathscr{L}'$ such that*

$$T \vdash \forall \boldsymbol{x}\, \exists \boldsymbol{y} \leqslant s(\boldsymbol{x})\, \theta(\boldsymbol{x}, \boldsymbol{y}).$$

Parikh proved this result for $I\Delta_0$ in [8] using a proof-theoretic argument. The model-theoretic argument of the full result is straightforward and well known, see for example the proof of Fact 4 on p. 127 of [1].

Other E_1 functions and ∇_1 relations in *IOpen* are listed below:

$\max(x, y)$,

$x \equiv y \bmod z$,

$$x \dot{-} y = \begin{cases} x - y & \text{if } x \geqslant y, \\ 0 & \text{otherwise,} \end{cases}$$

$\lfloor \sqrt{x} \rfloor$.

Slightly less trivial is the example $(x, y) = 1$ defined by

$$\forall z \leqslant x \, (z \mid x \wedge z \mid y \rightarrow z = 1) \wedge x > 0 \wedge y > 0.$$

Wilmers [12] shows that this is equivalent in IE_1 to

$$xy \geqslant 1 \wedge (x = 1 \vee y = 1 \vee (x < y \wedge \exists s < x \, (sy \equiv 1 \bmod x)) \vee (y < x \wedge \exists s < y \, (sx \equiv 1 \bmod y))).$$

If M is a model of PA^- and $p \in M$ we say that p is *irreducible* iff $M \models \forall x, y \, (p = xy \rightarrow (x = 1 \vee y = 1))$ and p is *prime* iff $M \models \forall x, y \, (p \mid xy \rightarrow (p \mid x \vee p \mid y))$. By Lemma 2.4 in [12] it follows that if $M \models IE_1$ and $p \in M$ then p is irreducible iff p is prime, and we shall refer to such numbers as 'primes'.

The function $p(x, y) = (x + y + 1)^2 + x$ will serve as a pairing function. Although it is not onto it has ∇_1 range defined by

$$x \in \text{range}(p) \overset{\text{def}}{\longleftrightarrow} (x - \lfloor \sqrt{x} \rfloor^2 < \lfloor \sqrt{x} \rfloor),$$

and given any $z \in \text{range}(p)$ we obtain the unique x, y such that $p(x, y) = z$ by the following E_1 functions in *IOpen*:

$$x = (z)_1 = z \dot{-} \lfloor \sqrt{z} \rfloor^2,$$

$$y = (z)_2 = \lfloor \sqrt{z} \rfloor \dot{-} (z)_1 \dot{-} 1.$$

A *diophantine* formula $\phi(\boldsymbol{x})$ is one of the form $\exists \boldsymbol{y} \, s(\boldsymbol{x}, \boldsymbol{y}) = r(\boldsymbol{x}, \boldsymbol{y})$ for polynomials r, s. A *bounded* diophantine formula is one of the form $\exists \boldsymbol{y} < t(\boldsymbol{x}) \, s(\boldsymbol{x}, \boldsymbol{y}) = r(\boldsymbol{x}, \boldsymbol{y})$ for polynomials r, s, t. The starting point for any study of Matijasevič's Theorem is the following:

Result 1.4. *In PA^-, any $\exists_1$ formula is equivalent to a diophantine formula and any E_1 formula is equivalent to a bounded diophantine formula.*

Proof. Let ϕ be $\exists_1$ and write it in prenex form with matrix in conjunctive normal form. Replace each $r(\boldsymbol{x}) > s(\boldsymbol{x})$ in this matrix by $\exists y < r(\boldsymbol{x})(r(\boldsymbol{x}) = s(\boldsymbol{x}) + 1 + y)$ and $r(\boldsymbol{x}) \neq s(\boldsymbol{x})$ by $\exists y < r(\boldsymbol{x}) + s(\boldsymbol{x})(r(\boldsymbol{x}) + y + 1 = s(\boldsymbol{x}) \vee s(\boldsymbol{x}) + y + 1 = r(\boldsymbol{x}))$. Replace $r_1(\boldsymbol{x}) = s_1(\boldsymbol{x}) \vee r_2(\boldsymbol{x}) = s_2(\boldsymbol{x})$ by the result of rearranging $(r_1(\boldsymbol{x}) - s_1(\boldsymbol{x})) \cdot (r_2(\boldsymbol{x}) - s_2(\boldsymbol{x})) = 0$ so that all terms are positive, and finally replace $r_1(\boldsymbol{x}) = s_1(\boldsymbol{x}) \wedge r_2(\boldsymbol{x}) = s_2(\boldsymbol{x})$ by the rearrangement of $(t_1(\boldsymbol{x}) - s_1(\boldsymbol{x}))^2 + (r_2(\boldsymbol{x}) - s_2(\boldsymbol{x}))^2 = 0$. □

Thus (modulo PA^-), 'diophantine induction' and 'bounded diophantine induction' are equivalent to $I\exists_1$ and IE_1 respectively.

In Section 6 we consider models of bounded diophantine induction. The following definitions and result are standard:

If $M_1 \subseteq M_2$ are models of PA^- we say M_1 is an *initial segment* of M_2 (written $M_1 \subseteq_e M_2$) iff $\forall a \in M_1\, \forall b \in M_2\, (M_2 \models b < a \Rightarrow b \in M_1)$. M_1 is *cofinal* in M_2 (written $M_1 \subseteq_{cf} M_2$) iff $\forall a \in M_2\, \exists b \in M_1\, (M_2 \models b \geqslant a)$. If Γ is a class of formulas we say M_1 is a *Γ-elementary substructure* of M_2 (written $M_1 \prec_\Gamma M_2$) iff for all $\gamma \in \Gamma$ and all $\boldsymbol{a} \in M_1$

$$M_1 \models \gamma(\boldsymbol{a}) \Leftrightarrow M_2 \models \gamma(\boldsymbol{a}).$$

$M_1 \prec_n M_2$ is understood to mean $M_1 \prec_{\Sigma_n} M_2$. By a simple induction on Δ_0 formulas we have:

Result 1.5. *If $M_1 \subseteq_e M_2$, then $M_1 \prec_0 M_2$.*

2. A diophantine function of exponential growth

Let $p(a, x, y) = x^2 + y^2 - 2axy - 1$. (The study of this polynomial is suggested by Julia Robinson's paper [9].)

Lemma 2.1. *In any model of PA^-, if $p(a, x, y) = 0 \wedge 0 < x \leqslant y \wedge a \geqslant 2$ then*

(i) $(2a-1)x \leqslant y \leqslant 2ax$,

(ii) $p(a, 2ax - y, x) = 0 \wedge 2ax - y \leqslant x$,

(iii) $p(a, y, 2ay - x) = 0 \wedge y \leqslant 2ay - x$.

Proof. Note that $y \neq 0$. To show (i), if $2ax < y$ then $1 = x^2 + y^2 - 2axy = x^2 - y(2ax - y) < x^2 - xy \leqslant 0$, contradiction. (ii) and (iii) follow by direct substitution. □

We write $\psi(a, b, x, y)$ for

$$p(a, x, y) = 0 \wedge x \leqslant y \wedge x \equiv b \bmod(a-1) \wedge y \equiv b + 1 \bmod(a-1).$$

Lemma 2.2. $I\exists_1 \vdash \forall a \geqslant 2\, \forall b \leqslant a - 2\, \exists u, v\, \psi(a, b, u, v)$.

Proof. By induction on b in

$$\theta(b) \overset{\text{def}}{=} (b \leqslant a - 2) \rightarrow \exists u, v\, \psi(a, b, u, v)$$

where a is any parameter $\geqslant 2$.

For $b = 0$, notice

$$p(a, 0, 1) = 0 \wedge 0 \equiv 0 \bmod a - 1 \wedge 1 \equiv 1 \bmod a - 1$$

so $\psi(a, 0, 0, 1)$ holds.

For the induction step, suppose

$$p(a, u, v) = 0 \wedge u \leqslant v \wedge u \equiv b \bmod a - 1 \wedge v \equiv b + 1 \bmod a - 1.$$

Then by 2.1, $u' = v$ and $v' = 2av - u$ satisfy $u' \leqslant v' \wedge p(a, u', v') = 0$. But also, $u' \equiv v \equiv b + 1 \bmod a - 1$ and $v' \equiv 2av - u \equiv 2a(b + 1) - b \equiv 2(a - 1)(b + 1) + 2(b + 1) - b \equiv b + 2 \bmod a - 1$ and so $\psi(a, b + 1, u', v')$ holds. Since $x \equiv y \bmod z$ is $\forall_1$ in *IOpen*, θ is $\exists_1$ and by $\exists_1$ induction we are done. □

The sentence in 2.2 is $\forall\exists$ and will be denoted E. We notice also that

Lemma 2.3. $I\Delta_0 + \exp \vdash E$.

Proof. By induction on b in

$$(b \leqslant a - 2) \rightarrow \exists u, v \leqslant (2a)^{a+1}(u \leqslant (2a)^b \wedge v \leqslant (2a)^{b+1} \wedge \psi(a, b, u, v))$$

for any fixed $a \geqslant 2$, using 2.1 again. □

Lemma 2.4. $IE_1 \vdash \forall a \geqslant 2\, \forall b \leqslant a - 2$

$$\forall u, v\, (\psi(a, b, u, v) \rightarrow \forall c \leqslant b\, \exists u', v' \leqslant v\, \psi(a, c, u', v')).$$

Proof. Fix a, b, u, v s.t. $\psi(a, b, u, v) \wedge b \leqslant a - 2 \wedge a \geqslant 2$ and consider

$$\theta(x) \overset{\text{def}}{=} \exists y \leqslant b\, (y + x = b \wedge \exists u', v' \leqslant v\, \psi(a, y, u', v')).$$

By IE_1 induction on x we show that $\forall x \leqslant b\, \theta(x)$. If $x = 0$, $u' = u$ and $v' = v$ will do. If $x < b$ then suppose $y = b - x \wedge \psi(a, y, u', v') \wedge y \neq 0$ so $0 < u' < v'$ since $u' \equiv y \bmod(a - 1)$, then by 2.1, $v' \leqslant 2au'$, $\psi(a, y - 1, 2au' - v', u')$ and $2au' - v' \leqslant u'$. The results now follows by IE_1 induction. □

Let $z = B(a, b)$ be the formula

$$\exists y \leqslant z\, \psi(a, b, y, z) \wedge \forall v < z\, \forall u \leqslant v\, \neg\psi(a, b, u, v).$$

Since $IE_1 \vdash LE_1$ we have

$$IE_1 \vdash \forall a, b\, (\exists y, z\, \psi(a, b, y, z) \rightarrow \exists z\, (z = B(a, b))).$$

Lemma 2.5. $IE_1 \vdash \forall a \geqslant 2\, \forall b \leqslant a - 2\, \forall z\, \forall c \leqslant b\, \forall u_1, u_2, v_1, v_2 \leqslant z$

$$[(z = B(a, b) \wedge \psi(a, c, u_1, v_1) \wedge \psi(a, c, u_2, v_2)) \rightarrow (u_1 = u_2 \wedge v_1 = v_2)].$$

Proof. Fix a, b, z s.t.

$$z = B(a, b) \wedge 2 \leqslant a \geqslant b + 2.$$

We show $\forall c \leqslant b\, \theta(c)$ by IU_1 induction on c, where $\theta(c)$ is

$$\forall u_1, u_2, v_1, v_2 \leqslant z\, [(\psi(a, c, u_1, v_1) \wedge \psi(a, c, u_2, v_2)) \rightarrow (u_1 = u_2 \wedge v_1 = v_2)].$$

If $c=0$ we must show $u_1=u_2=0 \wedge v_1=v_2=1$, but if $0<u_i \leqslant v_i \leqslant z \wedge \psi(a, c, u_i, v_i)$, then by 2.1, $\psi(a, a-2, 2au_i - v_i, u_i)$ and so by 2.4, $\exists x, y \leqslant u_i$ s.t. $\psi(a, b, x, y)$ contradicting $z = B(a, b)$.

For the induction step, if $c+1 \leqslant b < a$ and $\psi(a, c+1, u_i, v_i)$ for $i=1, 2$, then $\psi(a, c, 2au_i - v_i, u_i)$, $i=1, 2$, and so $\theta(c) \rightarrow u_1=u_2 \wedge v_1=v_2$ as required. □

Proposition 2.6. $IE_1 \vdash \forall a \geqslant 2\, \forall b \leqslant a-2\, \forall x, y$

$$[\psi(a, b, x, y) \rightarrow \forall a' \leqslant a\, \forall b' \leqslant \min(a' \dot{-} 2, b)$$
$$\exists u, v \leqslant y\, (a' \geqslant 2 \rightarrow \psi(a', b', u, v))].$$

Proof. Suppose $a \geqslant b+2 \wedge \psi(a, b, x, y) \wedge z = B(a, b)$. Clearly $z \leqslant y$. Fix a', b' with $2 \leqslant a' \leqslant a \wedge b' \leqslant \min(a'-2, b)$ and let $\theta(c)$ be

$$\exists u, v \leqslant z\, \exists u' \leqslant u\, \exists v' \leqslant v\, (\psi(a, c, u, v) \wedge \psi(a', c, u', v')).$$

We show $\forall c \leqslant \min(a'-2, b')\, \theta(c)$ by induction on θ. Clearly $\theta(0)$ holds. Suppose $\theta(c)$ holds with

$$u' \leqslant u \leqslant z \wedge v' \leqslant v \leqslant z \wedge \psi(a, c, u, v) \wedge \psi(a', c, u', v')$$

and $c+1 \leqslant \min(a'-2, b')$. Then $\psi(a, c+1, v, 2av-u)$ by 2.1 and $\exists x, y \leqslant z\, \psi(a, c+1, x, y)$ by 2.4 so by 2.5 we must have $v \leqslant 2av-u \leqslant z$ (for otherwise $\psi(a, c, 2ax-y, x)$ for some x, y with $(x \neq v \vee 2ax-y \neq u)$ and $2ax-y \leqslant x \leqslant z$). Thus $v' \leqslant v \leqslant z$ and $2a'v'-u' \leqslant 2av-u \leqslant z$ (if $a=a'$ this follows from $v=v' \wedge u=u'$ by 2.5 and if $a'+1 \leqslant a$ this follows from $2a'v'-u' \leqslant 2(a-1)v-u'$) with $\psi(a', c+1, v', 2a'u'-v')$ as required, completing the proof. □

Definition. $\mathscr{L}_Y$ is the language $\mathscr{L}$ expanded by adding a single binary function symbol Y. $IE_n(Y)$ is the theory in $\mathscr{L}_Y$ with nonlogical axioms:

(i) PA^-.

(ii) $\forall x\, (Y(0, x) = Y(1, x) = 1) \wedge \forall a \geqslant 2\, (Y(a, 1) = 2a)$,
$\forall a \geqslant 2\, \forall x\, (x \equiv 0 \bmod (a-1) \rightarrow Y(a, x) = 1)$,
$\forall a \geqslant 2\, \forall x\, (x+1 \not\equiv 0 \bmod (a-1) \rightarrow (2a-1)Y(a, x) \leqslant Y(a, x+1) \leqslant 2aY(a, x))$.

(iii) Induction on x for all E_n formulas $\theta(x, \boldsymbol{a})$ in the language $\mathscr{L}_Y$ such that whenever $Y(t, s)$ is a term in θ then neither x nor any quantified variables in θ may occur in t. (We do however allow the bounds in the quantifiers of θ to contain terms of the form $Y(t, s)$ provided that they obey this rule.)

To remind ourselves of the restriction in (iii) we shall write $Y(t, s)$ as $Y_t(s)$ and always ensure that t is a fixed parameter in the model we are working in.

Theorem 2.7. *For all $n \geqslant 1$, $IE_n(Y)$ is a conservative extension of $IE_n + E$.*

Proof. To show $IE_1(Y) \vdash E$ (and hence $IE_n(Y)$ is an extension of $IE_n + E$) fix an arbitrary $a \geq 2$ and show by induction on b using 2.1, that

$$\forall b < a-2\ \exists u, v \leq Y_{a+1}(b)\ \psi(a, b, u, v).$$

Let M be a model of $IE_n + E$. We show that there is an expansion M_Y of M to $\mathscr{L}_Y$. s.t. $M_Y \vDash IE_n(Y)$. Define Y in M as follows: If $a \leq 1$ then $Y_a(x) = 1$ for all x, and if $a \geq 2$ then $Y_a(x)$ is the unique $Y \in M$ such that

$$M \vDash Y \leq z \wedge \exists u \leq Y\ \psi\left(a, x - \left\lfloor \frac{x}{a-1} \right\rfloor \cdot (a-1), u, Y\right),$$

where $z = B(a, a-2)$, by 2.4 and 2.5. Clearly M_Y satisfies PA^- and the first two parts of (ii) above. If $a \geq 2$ and $x + 1 \not\equiv 0 \bmod (a-1)$ then

$$\psi\left(a, x+1 - \left\lfloor \frac{x+1}{a-1} \right\rfloor \cdot (a-1), Y_a(x), Y_a(x+1)\right),$$

so by 2.1(i) we have

$$(2a-1)Y_a(x) \leq Y_a(x+1) \leq 2aY_a(x).$$

To show M_Y satisfies the induction axioms in (iii) consider an E_n formula $\theta(x, \boldsymbol{a})$ of $\mathscr{L}_Y$, satisfying the restriction described there, for some (fixed) parameters $\boldsymbol{a} \in M$. By 1.4, θ is equivalent in M_Y to a formula of the form

$$\exists z_1 \leq t_1(x, \boldsymbol{a})\ \forall z_2 \leq t_n(x, \boldsymbol{a}) \cdots \exists z_n \leq t_n(x, \boldsymbol{a})\ r(x, \boldsymbol{a}, \boldsymbol{z}) = s(x, \boldsymbol{a}, \boldsymbol{z})$$

if n is odd; and to a formula of the form

$$\exists z_1 \leq t_1(x, \boldsymbol{a})\ \forall z_2 \leq t_n(x, \boldsymbol{a}) \cdots \forall z_n \leq t_n(x, \boldsymbol{a})\ r(x, \boldsymbol{a}, \boldsymbol{z}) \neq s(x, \boldsymbol{a}, \boldsymbol{z})$$

if n is even. Here $\boldsymbol{z}_i$ is $z_{i1} \cdots z_{in_i}$, the quantifier blocks alternate in type and t_i, s, r are terms of $\mathscr{L}_Y$ such that for no subterm $Y_u(v)$ does u contain x or any z_{ij}.

Fix an arbitrary $c \in M$ and find $\tau_i \geq t_i(x, \boldsymbol{a})$, $\alpha \geq \max(r(c, \boldsymbol{a}, \boldsymbol{z}), s(c, \boldsymbol{a}, \boldsymbol{z}), \boldsymbol{\tau})$ for all $x \leq c$ and all $\boldsymbol{z}_i \leq \tau_i$ so that for all subterms $u(x, \boldsymbol{a}, \boldsymbol{z})$ of θ, all $x \leq c$ and all $\boldsymbol{z}_i \leq t_i(x, \boldsymbol{a})$ we have $u(x, \boldsymbol{a}, \boldsymbol{z}) \leq \alpha$. (For example, suitable τ_i can be obtained from the t_i by replacing each $Y_u(v)$ in t_i by $Y_u(u-2)$ and each x by c, using the condition on subterms $Y_u(v)$ described above and the fact that in M_Y, $Y_u(u-2) \geq Y_u(x)$ for all u, x. α can be found from the $\boldsymbol{\tau}$ and r, s in a similar way.) Now for all subterms $u(x, \boldsymbol{a}, \boldsymbol{z})$ of θ define the formula $(y = u(x, \boldsymbol{a}, \boldsymbol{z}))^*$ by (meta) induction as follows:

(i) If u is a constant, variable or parameter $(y = u)^*$ is just $y = u$.

(ii) If u is $u_1 \circ u_2$ (where $\circ$ is $+$ or $\cdot$) then $(y = u)^*$ is

$$\exists y', y'' \leq \alpha\ ((y' = u_1)^* \wedge (y'' = u_2)^* \wedge (y' \circ y'' = y))$$

where y', y'' are new variables.

(iii) If u is $Y_{u_1}(u_2)$ with u_1 a term containing only parameters from M_Y and constants, let $d, b \in M_Y$ satisfy

$$M_Y \vDash u_1 = b \wedge d = B(b, b-2)$$

and let $(y = u)^*$ be

$$y \leqslant d \wedge \exists y' \leqslant y \, \exists y'' \leqslant \alpha \left[(y'' = u_2)^* \wedge \psi\left(b, y'' - \left\lfloor \frac{y''}{b-1} \right\rfloor, y', y\right)\right].$$

By (meta) induction on terms we can show that for all y, $x \leqslant c$, $z_i \leqslant t_i(x, \boldsymbol{a})$,

$$M_Y \vDash y = u(x, \boldsymbol{a}, z) \Leftrightarrow M \vDash (y = u(x, \boldsymbol{a}, z))^*$$

and that $(y = u)^*$ is E_1 in $\mathscr{L}$.

Notice that $(y = u)^*$ may contain many new parameters from M not in u. For simplicity we have omitted them from the notation.

Let $\theta^*(x, \boldsymbol{a})$ be

$$\exists w_1 \leqslant \tau_1 \, \exists z_1 \leqslant \tau_1 \, \forall w_2 \leqslant \tau_2 \, \forall z_2 \leqslant \tau_2 \cdots \exists w_n \leqslant \tau_n \, \exists z_n \leqslant \tau_n \, \exists y_1, y_2 \leqslant \alpha$$

$$\left[\bigwedge_{k \text{ even}} \left((w_k = t_k(x, \boldsymbol{a}))^* \wedge \bigwedge_j z_{kj} \leqslant w_k \right) \rightarrow \left[\bigwedge_{k \text{ odd}} \left((w_k = t_k(x, \boldsymbol{a}))^* \right.\right.\right.$$

$$\left.\left.\left. \wedge \bigwedge_j z_{kj} \leqslant w_k \right) \wedge (y_1 = r(x, \boldsymbol{a}, z))^* \wedge (y_2 = s(x, \boldsymbol{a}, z))^* \wedge y_1 = y_2 \right] \right]$$

in the case n odd, a similar formula if n is even. So θ^* is E_n in $\mathscr{L}$ and we may check that for all $x \leqslant c$

$$M_Y \vDash \theta(x, \boldsymbol{a}) \Leftrightarrow M \vDash \theta^*(x, \boldsymbol{a}).$$

It then follows from the following instance of IE_n in M,

$$M \vDash \theta^*(c, \boldsymbol{a}) \vee \neg\theta^*(0, \boldsymbol{a}) \vee \exists x < c \, (\theta^*(x, \boldsymbol{a}) \wedge \neg\theta^*(x+1, \boldsymbol{a}))$$

that

$$M_Y \vDash \theta(c, \boldsymbol{a}) \vee \neg\theta(0, \boldsymbol{a}) \vee \exists x < c \, (\theta(x, \boldsymbol{a}) \wedge \neg\theta(x+1, \boldsymbol{a})),$$

and so since c was arbitrary, $M_Y \vDash IE_n(Y)$. □

Notice that in any model $M \vDash IE_1(Y)$ and for any $n \in \mathbb{N}$, $a \in M$ with $m \vDash 0 < n < a$ we have $M \vDash Y_a(0) = 1$ and

$$M \vDash (2a-1)^n \leqslant Y_a(n) < (2a)^n.$$

Thus the function $Y_a(n)$ is of 'exponential growth'. We will eventually show that these inequalities hold even for nonstandard n, but to do this we will first have to define exponentiation in $IE_1(Y)$.

3. Definition of exponentiation in $IE_1(Y)$

In Section 2 we show that, rather than working in $IE_1 + E$, we might as well work in $IE_1(Y)$. The Y function is still rather unwieldy, so our next task therefore is to define 2^x and x^y.

Working in PA^- for the moment, suppose $a \geqslant 2$. Then $a^2 \leqslant a^2 + a - 2 = a(a-1) + 2(a-1)$. We may write this result in a more suggestive way using fractions as

$$\left(1 - \frac{1}{a}\right)^{-1} = \frac{a}{a-1} \leqslant 1 + \frac{2}{a}.$$

Now although the division symbol is not in our language, we may agree always to interpret expressions such as that above by 'multiplying them out', in this case as $a^2 \leqslant a(a-1) + 2(a-1)$. We shall adopt this convention from now on. The reader may check that the 'correct' expression always has the same quantifier complexity.

Let $\chi(a, m, n, z)$ be the formula

$$z \leqslant \max\left(\frac{Y_m(n)}{2}, 1\right) \wedge z - \frac{nY_m(n)}{a} \leqslant \frac{Y_{am}(n)}{Y_a(n)} \leqslant z + \frac{nY_m(n)}{a}.$$

The idea is that, for sufficiently large a, m, $\chi(a, m, n, z)$ represents $m^n = z$ in $IE_1(Y)$.

Lemma 3.1. *In $IE_1(Y)$, if $a > 2$ and $m > 2$ then*

(i) $\chi(a, m, 0, 1)$ *and*

(ii) $\forall z\, \forall n < m - 2\, (\chi(a, m, n, z) \rightarrow \chi(a, m, n+1, mz))$.

Proof. (i) $Y_a(0) = Y_{am}(0) = 1$ so

$$\frac{Y_{am}(0)}{Y_a(0)} = 1.$$

(ii) Suppose $n < m - 2$ and $\chi(a, m, n, z)$. Then,

$$\begin{aligned}
\frac{Y_{am}(n+1)}{Y_a(n+1)} &\leqslant \frac{2am}{2a-1} \cdot \frac{Y_{am}(n)}{Y_a(n)} \\
&\leqslant m\left(1 - \frac{1}{2a}\right)^{-1}\left\{z + \frac{nY_m(n)}{a}\right\} \\
&\leqslant m\left(1 + \frac{1}{a}\right)\left\{z + \frac{nY_m(n)}{a}\right\} \\
&\leqslant mz + \frac{nmY_m(n)}{a} + \frac{mz}{a} + \frac{nmY_m(n)}{a^2}.
\end{aligned}$$

Now if $n = 0$ then $z = 1$ and $mz/a = m/a \leqslant Y_m(1)/a$ and if $n > 0$ then $z \leqslant Y_m(n)/2$ and,

$$\begin{aligned}
\frac{Y_{am}(n+1)}{Y_a(n+1)} &\leqslant mz + nmY_m(n) \cdot \left\{\frac{1}{a} + \frac{1}{2na} + \frac{1}{a^2}\right\} \\
&\leqslant mz + \frac{n+1}{a} Y_m(n+1).
\end{aligned}$$

(This last step is by considering the two cases $n = 1$ and $n > 1$ using $Y_m(1) = 2m$.)
Also,

$$\frac{Y_{am}(n+1)}{Y_a(n+1)} \geqslant \frac{2am-1}{2a} \cdot \frac{Y_{am}(n)}{Y_a(n)}$$
$$\geqslant \left(m - \frac{1}{2a}\right)\left\{z - \frac{nY_m(n)}{a}\right\}$$
$$\geqslant mz - \frac{z}{2a} - \frac{nmY_m(n)}{a} + \frac{nY_m(n)}{2a^2}.$$

So once again, if $n = 0$ and $z = 1$ then this is $\geqslant mz - 1/2a \geqslant mz - (n+1)Y_m(n+1)/a$, and if $n > 0$ then $z \leqslant Y_m(n)/2$ so,

$$\frac{Y_{am}(n+1)}{Y_a(n+1)} \geqslant mz - \frac{Y_m(n)}{4a} - \frac{nmY_m(n)}{a}$$
$$\geqslant mz - \frac{(n+1)Y_m(n+1)}{a}.$$

To complete the proof we must show that $mz \leqslant Y_m(n+1)/2$. If n is 0 and z is 1 this follows from $Y_m(1) = 2m$, and otherwise $z \leqslant Y_m(n)/2$, so

$$mz \leqslant \frac{mY_m(n)}{2} \leqslant \frac{m}{2m-1} \cdot \frac{Y_m(n+1)}{2} \leqslant \frac{Y_m(n+1)}{2}. \qquad \square$$

We can now define the function $Z_{a,m}(x)$, which, for sufficiently large a, m, represents m^x.

Definition

$$Z_{a,m}(x) = \left\lfloor \frac{Y_{am}(x)}{Y_a(x)} + \frac{1}{2} \right\rfloor.$$

Once again we use the subscript notation $Z_{a,m}(x)$ to remind ourselves that no variable occurring in a or m may be the induction variable or a quantified variable in an instance of an induction axiom. Immediately from 3.1 and the definition we have:

Lemma 3.2. (i) $IE_1(Y) \vdash \forall a, m, x\ \exists! z\ (z = Z_{a,m}(x))$.
(ii) $IE_1(Y) \vdash \forall m > 2\ \exists b\ \forall a \geqslant b\ (Z_{a,m}(0) = 1 \wedge \forall x < m - 2\ \forall z\ (Z_{a,m}(x) = z \rightarrow Z_{a,m}(x+1) = mz))$.

Proof. (i) is obvious. For (ii), given $m > 2$ choose any $a \geqslant 2(m-2)Y_m(m-2) + 1$. We can show that $\forall x \leqslant m - 2\ (xY_m(x)/a < 1/2)$ by a simple induction on x. Now once again by induction on x using 3.1 we see that

$$\forall x \leqslant m - 2\ \chi(a, m, x, Z_{a,m}(x)).$$

Indeed $\chi(a, m, 0, Z_{a,m}(0))$ and $\chi(a, m, x, Z_{a,m}(x)) \rightarrow \chi(a, m, x+1, mZ_{a,m}(x))$ so

$$mZ_{a,m}(x) - \frac{(x+1)Y_m(x+1)}{a} \leqslant \frac{Y_{am}(x+1)}{Y_a(x+1)} \leqslant mZ_{a,m}(x) + \frac{(x+1)(Y_m(x+1)}{a}$$

from which it follows that $mZ_{a,m}(x) = Z_{a,m}(x+1)$ and we are done. □

The next function $l_{a,b}(x)$ represents 2^x provided x is sufficiently small compared with a, b.

Definition. $l_{a,b}(x) = y$ is the formula

$$\exists u, v\ (u = Z_{a,2b}(x) \wedge v = Z_{a,b}(x) \wedge yv = u).$$

Proposition 3.3. $IE_1(Y) \vdash \forall y\ \exists a, b$

$$[\forall x \leqslant y\ \exists! z\ l_{a,b}(x) = z \wedge \forall z\ \forall x < y\ (l_{a,b}(x) = z \rightarrow l_{a,b}(x+1) = 2z) \wedge l_{a,b}(0) = 1].$$

Proof. Given y, fix $b \geqslant y + 2$ and a such that

$$Z_{a,m}(0) = 1 \wedge \forall x < y\ Z_{a,m}(x+1) = mZ_{a,m}(x)$$

for $m =$ both b and $2b$, by 3.2.

We now prove by induction on x that $\forall x \leqslant y\ (Z_{a,b}(x) \mid Z_{a,2b}(x))$. Indeed $Z_{a,b}(0) = 1$ divides $Z_{a,2b}(0) = 1$ and for $x < y$, $Z_{a,b}(x+1) = bZ_{a,b}(x)$, $Z_{a,2b}(x+1) = 2bZ_{a,2b}(x)$ so if $Z_{a,b}(x) \mid Z_{a,2b}(x)$ then $Z_{a,b}(x+1) \mid Z_{a,2b}(x+1)$. Hence,

$$\forall x \leqslant y\ \exists! z\ l_{a,b}(x) = z.$$

It is clear that $l_{a,b}(0) = 1$. Suppose $x < y$, $l_{a,b}(x) = z$, $u = Z_{a,2b}(x)$ and $v = Z_{a,b}(x)$. Then $zv = u$ and $Z_{a,b}(x+1) = bv$, $v = Z_{a,2b}(x+1) = 2bu$, so

$$2zZ_{a,b}(x+1) = Z_{a,2b}(x+1)$$

hence $2z = l_{a,b}(x+1)$ and we are done. □

Definition. $IE_n(2^x)$ is the theory in the language $\mathcal{L}_{\exp}$, which is $\mathcal{L}$ together with a single unary function symbol 2^x, consisting of the following nonlogical axioms:

(i) PA^-;

(ii) $2^0 = 1 \wedge \forall x\ (2^{x+1} = 2 \cdot 2^x)$;

(iii) induction for all E_n formulas in the language $\mathcal{L}_{\exp}$.

Theorem 3.4. *For all $n \geqslant 1$, $IE_n(2^x)$ is a conservative extension of $IE_n + E$.*

Proof. (We leave the reader to check that $IE_n(2^x) \vdash E$.) Let $M \models IE_n + E$ and define $Y_a(b)$ in M as in 2.7. For each $y \in M$, define 2^x for all $x \leqslant y$ by $2^x = l_{a,b}(x)$ for suitable a, b using 3.3. A simple induction in M shows that this is well defined, and clearly satisfies (ii) above. Now mimic the proof of 2.7 to show that the resulting structure satisfies $IE_n(2^x)$. □

Next we show how to define x^y in $IE_1(2^x)$. The trick we use is due to Julia Robinson, communicated to me by J.P. Jones.

Definition. $x^y = z$ is the formula

$$(z < 2^w - x) \wedge (z \equiv 2^{wy} \bmod 2^w - x),$$

where $w = xy + x + 1$.

Clearly, in models of $IE_1(2^x)$, we have $2^w > x$ for $w = xy + x + 1$, so that

$$IE_1(2^x) \vdash \forall x, y\ \exists! z\ (x^y = z).$$

Proposition 3.5. *$IE_1(2^x)$ proves*:

(i) $\forall y > 0\ (0^y = 0)$,

(ii) $\forall x\ (x^0 = 1)$,

(iii) $\forall x, y, z\ (x^y = z \rightarrow x^{y+1} = xz)$.

Proof. (i) By induction we can show that $\forall y > 0\ (2^y \equiv 0 \bmod 2)$. If $w = xy + x + 1$ and $x = 0$ then $w = 1$, $0 < 2^w - x = 2$ and so

$$0 \equiv 2^{wy} \bmod 2 \quad \text{for all } y > 0.$$

(ii) If $w = x + 1$ then by induction we can show that $\forall x\ (1 < 2^w - x)$. But if $y = 0$ then $2^{wy} = 1$ and $1 \equiv 2^{wy} \bmod 2^w - x$, hence $x^0 = 1$.

(iii) Let

$$\theta(x, y, z, a) \overset{\text{def}}{=} (z < 2^{xy+x+1} - x \wedge z \equiv 2^{ay} \bmod 2^a - x).$$

Then for any $a \geqslant xu + x + 1$ and $u > y$, since $x \equiv 2^a \bmod 2^a - x$ we have

$$\forall z\ (\theta(x, y, z, a) \rightarrow \theta(x, y + 1, xz, a)) \qquad (*)$$

and also $\forall y \leqslant u\ \exists! z\ \theta(x, y, z, a)$.

Now if $b > a \geqslant xu + x + 1$ we show by induction on y that

$$\forall y \leqslant u\ \forall z \leqslant a\ (\theta(x, y, z, a) \rightarrow \theta(x, y, z, b)).$$

Indeed for $y = 0$, $\theta(x, 0, z, a) \rightarrow z = 1 \rightarrow \theta(x, 0, z, b)$, and for $y > 0$, suppose $\theta(x, y, z, a)$ and $z' \leqslant a$ satisfies $\theta(x, y - 1, z', a)$, then $z = xz'$ and $\theta(x, y - 1, z', b)$ by the induction hypothesis. Hence by $(*)$ $\theta(x, y, xz', b)$ and we are done. Putting $a = xy + x + 1$ and $b = x(y + 1) + x + 1$ gives as a special case of this

$$x^y = z \rightarrow \theta(x, y, z, x(y + 1) + x + 1),$$

and another application of $(*)$ then gives $x^y = z \rightarrow x^{y+1} = xz$ as required. □

We conclude this section by showing how to define $\binom{x}{y}$ and $x!$ in $IE_1(2^x)$.

Definition. The formula $z = \binom{n}{m}$ is

$$\exists y \leqslant (1 + x)^n \left[z < x \wedge xy + z \leqslant \frac{(1 + x)^n}{x^m} < xy + z + 1 \right]$$

where $x = (2(n+1)(m+1))^{m+1}$. Thus $\binom{n}{m}$ is the remainder on dividing

$$\lfloor (1+x)^n / x^m \rfloor$$

by x.

Clearly then,

$$IE_1(2^x) \vdash \forall m, n\ \exists! z\ z = \binom{n}{m}.$$

To show $\binom{n}{m}$ as defined above has all the usual properties we first need the following:

Lemma 3.6. $IE_1(2^x) \vdash$

(i) $\forall a, n\ (a \geqslant n \rightarrow (1 + 1/a)^n \leqslant 1 + 2n/a)$,

(ii) $\forall a > 1\ \forall n\ (1 \equiv (1+a)^n \bmod a)$.

Proof. Both are proved by induction on n for a fixed parameter a. □

Proposition 3.7. $IE_1(2^x) \vdash$

(i) $\forall n \binom{n}{0} = 1$,

(ii) $\forall n, m \left(m > n \rightarrow \binom{n}{m} = 0\right)$,

(iii) $\forall n, m \left(\binom{n+1}{m} = \binom{n}{m} + \binom{n}{m+1}\right)$.

Proof. Let $\phi(n, m, y, z, a)$ be the formula

$$z < a \wedge \left(ay + z \leqslant \frac{(1+a)^n}{a^m} < ay + z + \frac{2mn^m}{a}\right).$$

Fix an arbitrary x_0. We show by induction on k that $\forall k\ \psi(k, x_0)$ where ψ is

$$\forall n, m \leqslant k\ \forall x \leqslant x_0\ \forall y, z \leqslant (1+x)^n$$
$$\left[\left(n + m \leqslant k \wedge x \geqslant (2(n+1)(m+1))^{m+1}\right.\right.$$
$$\left.\left. \wedge\ y = \left\lfloor \left\lfloor \frac{(1+x)^n}{x^m} \right\rfloor \Big/ x \right\rfloor \wedge z = \binom{n}{m}\right) \rightarrow \phi(n, m, y, z, x)\right].$$

If $m = 0$ and $x \geqslant 2(n+1) \geqslant 2$ then $(1+x)^n = xy + 1$ for $y = \lfloor (1+x)^n / x \rfloor$ by 3.6(ii), and so we see that $\binom{n}{0} = 1$ and $\phi(n, 0, \lfloor (1+x)^n/x \rfloor, \binom{n}{0}, x)$ hold.

If $n < m$ and $x \geqslant (2(n+1)(m+1))^{m+1}$ then

$$0 \leqslant \frac{(1+x)^n}{x^m} < \frac{\left(1 + \frac{1}{x}\right)^n}{x^{m-n}} < \left(1 + \frac{2n}{x}\right) \cdot \frac{1}{x} \leqslant \frac{2n}{x}$$

by 3.6(i) and $2n/x \leqslant 2mn^m/x$ so $\binom{n}{m} = 0$ and

$$\phi\left(n, m, \left\lfloor \left\lfloor \frac{(1+x)^n}{x^m} \right\rfloor / x \right\rfloor, \binom{n}{m}, x\right).$$

Now for the induction step: suppose $\psi(k, x_0)$ holds, that $n + m \leqslant k + 1$, $x \leqslant x_0$ with $x \geqslant (2(n+1)(m+1))^{m+1}$,

$$y_0 = \left\lfloor \left\lfloor \frac{(1+x)^n}{x^m} \right\rfloor / x \right\rfloor \quad \text{and} \quad z_0 = \binom{n}{m}.$$

We must show $\phi(n, m, y_0, z_0, x)$. By the above, we may assume $n > 0$ and $m \leqslant n$. Notice that

$$\frac{(1+x)^n}{x^m} = \frac{(1+x)^{n-1}}{x^{m-1}} + \frac{(1+x)^{n-1}}{x^m} \tag{†}$$

with $(n-1) + (m-1)$ and $(n-1) + m$ both $\leqslant k$. So by $\psi(k, x_0)$ we have

$$\forall x \leqslant x_0 \left[x \geqslant (2(n+1)(m+1))^{m+1} \rightarrow \right.$$

$$\left. \left(\phi\left(n-1, m-1, y_1(x), \binom{n-1}{m-1}, x\right) \wedge \phi\left(n-1, m, y_2(x), \binom{n-1}{m}, x\right)\right)\right]$$

where

$$y_1(x) = \left\lfloor \left\lfloor \frac{(1+x)^{n-1}}{x^{m-1}} \right\rfloor / x \right\rfloor \quad \text{and} \quad y_2(x) = \left\lfloor \left\lfloor \frac{(1+x)^{n-1}}{x^m} \right\rfloor / x \right\rfloor,$$

hence by (†) above for all such x

$$x(y_1(x) + y_2(x)) + \binom{n-1}{m-1} + \binom{n-1}{m} \leqslant \frac{(1+x)^n}{x^m}$$

$$\leqslant x(y_1(x) + y_2(x)) + \binom{n-1}{m-1} + \binom{n-1}{m} + \frac{2(m-1)(n-1)^{m-1}}{x} + \frac{2m(n-1)^m}{x}$$

with (from the definition of $\binom{a}{b}$)

$$\binom{n-1}{m-1} + \binom{n-1}{m} < (2mn)^m + (2(m+1)n)^{m+1} \leqslant (2(m+1)(n+1))^{m+1}$$

and hence,

$$\binom{n-1}{m-1} + \binom{n-1}{m} < x.$$

Also,

$$\frac{2(m-1)(n-1)^{m-1}}{x} + \frac{2m(n-1)^m}{x} \leqslant \frac{2mn^m}{x} < 1$$

so we conclude that

$$y_1(x)+y_2(x)=\left\lfloor\left\lfloor\frac{(1+x)^n}{x^m}\right\rfloor\Big/x\right\rfloor=y_0$$

for all x in the range $(2(m+1)(n+1))^{m+1}\leqslant x\leqslant x_0$, and also, for all such x,

$$\phi\left(n, m, y_1(x)+y_2(x), \binom{n-1}{m-1}+\binom{n-1}{m}, x\right).$$

Putting $x=(2(m+1)(n+1))^{m+1}$ we see from this that

$$\binom{n-1}{m-1}+\binom{n-1}{m}=\binom{n}{m}=z_0$$

and hence $\phi(n, m, y_0, z_0, x)$ as required, completing the induction step and the proof of the proposition. □

Proposition 3.8. $IE_1(2^x)\vdash$

(i) $\forall n, m\left[n+1>m\rightarrow\binom{n+1}{m}=\frac{n+1}{n+1-m}\binom{n}{m}\right]$,

(ii) $\forall n, m\left[\binom{n}{m+1}=\frac{n-m}{m+1}\binom{n}{m}\right]$.

Proof. By induction on k in

$$\forall m, n\leqslant k\left\{m+n\leqslant k\rightarrow\left[\binom{n}{m+1}=\frac{n-m}{m+1}\binom{n}{m}\right.\right.$$
$$\left.\left.\wedge\left(n+1>m\rightarrow\binom{n+1}{m}=\frac{n+1}{n+1-m}\binom{n}{m}\right)\right]\right\}.$$

If $m=n=0$ then as $\binom{0}{1}=0$ and $\binom{1}{0}=1$ this works. For the induction step, suppose $m+n\leqslant k+1$.

If $n+1>m$ we must show that

$$\binom{n+1}{m}=\frac{n+1}{n+1-m}\binom{n}{m}.$$

If $m=0$, as $\binom{n+1}{0}=1$, there's nothing to do. If $m=b+1$ then by the induction hypothesis

$$\binom{n+1}{m}=\binom{n}{b}+\binom{n}{b+1}$$
$$=\binom{n}{b+1}\left\{\frac{b+1}{n-b}+1\right\}=\frac{n+1}{n+1-m}\binom{n}{m}$$

as required.

To show

$$\binom{n}{m+1} = \frac{n-m}{m+1}\binom{n}{m},$$

suppose $n \geqslant m+1$ (for if $n < m+1$ either $n = m$ or $\binom{n}{m} = 0$ and there's nothing to do). Write $n = b+1$ where $b \geqslant m$, and using the induction hypothesis twice we have

$$\begin{aligned}\binom{n}{m+1} &= \binom{b}{m} + \binom{b}{m+1} \\ &= \binom{b}{m}\left\{1 + \frac{b-m}{m+1}\right\} = \frac{b+1}{m+1}\binom{b}{m} \\ &= \frac{b+1}{m+1}\cdot\frac{b+1-m}{b+1}\binom{b+1}{m} = \frac{n-m}{m+1}\binom{n}{m}\end{aligned}$$

as required. □

Definition. $r! = z$ is the formula

$$\left(r > 0 \wedge z \leqslant x^r \Big/ \binom{x}{r} < z+1\right) \vee (r = 0 \wedge z = 1)$$

where x is $2r^{r+2}+1$. Hence $IE_1(2^x) \vdash \forall r\, \exists! z\, r! = z$. Since $\binom{x}{1} = x$ for $x \geqslant 2$, we see that $1! = 1$.

Proposition 3.9. $IE_1(2^x) \vdash \forall r\, ((r+1)! = r! \cdot (r+1))$.

Proof. We show by induction on r that $\forall r > 0\ \phi(r, a_0)$ where $\phi(r, a_0)$ is

$$r! \leqslant r^r \wedge \forall a \leqslant a_0 \left[a > 2r^{r+2}+1 \rightarrow r! \leqslant a^r \Big/ \binom{a}{r} \leqslant r! + \frac{2r^{r+2}}{a}\right]$$

and a_0 is any fixed parameter.

For $r = 1$ we have seen that $r! = 1$, so $a^r = \binom{a}{r} = a$ for $a \geqslant 1$, and we are done.

For the induction step, suppose $\phi(r, a_0)$ holds with $r \geqslant 1$ and $a_0 \geqslant a \geqslant 2(r+1)^{r+3}$. Then,

$$r! \leqslant a^r \Big/ \binom{a}{r} \leqslant r! + \frac{2r^{r+2}}{a}$$

and by 3.8,

$$a^{r+1} \Big/ \binom{a}{r+1} = (r+1)\cdot\frac{a}{a-r}\cdot a^r \Big/ \binom{a}{r}$$

so,

$$a^{r+1} \Big/ \binom{a}{r+1} \geqslant (r+1)\cdot r!$$

and

$$a^{r+1}\Big/\binom{a}{r+1} \leqslant (r+1)\left(1-\frac{r}{a}\right)^{-1}\left\{r!+\frac{2r^{r+2}}{a}\right\}$$
$$\leqslant (r+1)\left(1+\frac{2r}{a}\right)\left\{r!+\frac{2r^{r+2}}{a}\right\}$$
$$\leqslant (r+1)\cdot r!+(r+1)\left\{\frac{2r\cdot r!}{a}+\frac{4r\cdot r^{r+2}}{a^2}+\frac{2r^{r+2}}{a}\right\}$$
$$\leqslant (r+1)\cdot r!+\frac{2(r+1)^{r+3}}{a}$$

(using $r! \leqslant r^r$). Putting $a = 2(r+1)^{r+3}+1$ we see that $(r+1)\cdot r! = (r+1)!$ and hence

$$(r+1)! \leqslant (r+1)r^r \leqslant (r+1)^{r+1}$$

completing the induction step and the proof. □

The following property of the factorial function will be useful later:

Proposition 3.10. $IE_1(2^x) \vdash \forall r\, \forall y \leqslant r\, \forall n \leqslant r\, (y \neq 0 \wedge ny \leqslant r \rightarrow y^n \mid r!)$.

Proof. Induction on r. □

4. Matijasevič's Theorem

For Lemmas 4.1 to 4.8, work in $IE_1(2^x)$ with two fixed numbers Q, y satisfying $Q > 2y > y > 0$.

Lemma 4.1. *Suppose* $1 \leqslant k \leqslant y$. *Then*

$$\left(\frac{Q!}{k}-1\right) \Big| \binom{Q!-1}{y}.$$

Proof. By 3.10, $k \mid Q!$ and $Q!/k > 1$. We show by induction on y that

$$\forall y < Q\left[\forall k < y\left(\frac{Q!}{k+1}-1\right) \Big| \binom{Q!-1}{y}\right].$$

If $y > 0$ then by 3.8(ii) we have

$$\binom{Q!-1}{y} = \left(\frac{Q!}{y}-1\right)\cdot\binom{Q!-1}{y-1},$$

so if $k = y-1$ then

$$\left(\frac{Q!}{k+1}-1\right) \Big| \binom{Q!-1}{y},$$

and if $k < y - 1$ then

$$\left(\frac{Q!}{k+1} - 1\right) \Big| \binom{Q!-1}{y-1} \Big| \binom{Q!-1}{y}$$

by the induction hypothesis. □

Lemma 4.2. *If p is prime and*

$$y > z \geqslant 0 \wedge p \Big| \left(\frac{Q!}{z+1} - 1\right)$$

then $p > Q$.

Proof. Otherwise $p \mid Q! - (z+1)$ and by 3.10, $p \leqslant Q \rightarrow p \mid Q!$, so $p \leqslant Q \rightarrow p \mid z+1$. But $Q > 2y$ so by (2.10) again $(z+1)^2 \mid Q!$, so if $p \leqslant Q$ we have $p \mid Q!/(z+1)$ and hence $p = 1$, contradiction. □

Lemma 4.3. *If $y > w > z \geqslant 0$ then*

$$\left(\frac{Q!}{z+1} - 1, \frac{Q!}{w+1} - 1\right) = 1.$$

Proof. Otherwise for some prime p,

$$p \mid Q! - (z+1) \quad \text{and} \quad p \mid Q! - (w+1)$$

hence $p \mid (w - z) < y < Q$, contradicting 4.2. □

Lemma 4.4. *If $z < y$ then*

$$Q! - 1 \equiv z \bmod \left(\frac{Q!}{z+1} - 1\right).$$

Proof.

$$Q! - 1 = z + (z+1)\left(\frac{Q!}{z+1} - 1\right). \qquad \square$$

Lemma 4.5. *If p is prime and $p \mid v!\binom{b}{v}$ where $b > v > 0$ then*

$$\exists x < v\,(p \mid (b - x)).$$

Proof. By induction on v. If $v = 1$, $1!\binom{b}{1} = b$ so $p \mid b$ and we may put $x = 0$. Otherwise,

$$(v+1)!\binom{b}{v+1} = (v+1) \cdot v! \cdot \frac{b-v}{v+1}\binom{b}{v}$$

$$= (b - v) \cdot v!\binom{b}{v},$$

using 3.8(ii) and 3.9, and so $p \mid b - v$ or $p \mid v!\binom{b}{v}$, so in the second case there is $x < v$ with $p \mid (b - x)$ as required. □

Lemma 4.6. *For all* $z, w < y$

$$\left[z > w \to \left(\binom{Q!-1}{w+1}, \frac{Q!}{z+1} - 1\right) = 1\right]$$
$$\wedge \left[z \leqslant w \to \left(\frac{Q!}{z+1} - 1\right) \mid \binom{Q!-1}{w+1}\right].$$

Proof. The second part follows from 4.1. We show the first by induction on w.
If $0 = w < z$ then

$$\binom{Q!-1}{w+1} = Q! - 1 = \frac{Q!}{0+1} - 1$$

which is coprime to $Q!/(z+1) - 1$ by 4.3. Otherwise, if $w + 1 < z$,

$$\binom{Q!-1}{w+1+1} = \frac{Q! - 1 - (w+1)}{w+2}\binom{Q!-1}{w+1} \quad \text{by 3.8(ii)}$$
$$= \left(\frac{Q!}{w+2} - 1\right)\binom{Q!-1}{w+1}$$

and by 4.3, $Q!/(w+2) - 1$ and $Q!/(z+1) - 1$ are coprime, and by the induction hypothesis

$$\binom{Q!-1}{w+1} \quad \text{and} \quad \frac{Q!}{(z+1)} - 1$$

are coprime, hence

$$\left(\binom{Q!-1}{w+2}, \frac{Q!}{z+1} - 1\right) = 1$$

as required. □

Lemma 4.7. *If* $1 \leqslant w \leqslant y$ *and*

$$\forall z < w \; a \equiv b \bmod\left(\frac{Q!}{z+1} - 1\right)$$

then

$$a \equiv b \bmod\binom{Q!-1}{w}.$$

Proof. By induction on w. For $w = 1$,

$$\binom{Q!-1}{w} = Q! - 1$$

so there is nothing to prove. Otherwise,

$$\binom{Q!-1}{w+1} = \left(\frac{Q!}{w+1} - 1\right)\binom{Q!-1}{w}$$

hence if $\forall z < w+1\ a \equiv b \bmod(Q!/(z+1)-1)$ we have

$$a \equiv b \bmod\left(\frac{Q!}{w+1} - 1\right)$$

and,

$$a \equiv b \bmod\binom{Q!-1}{w}$$

by the induction hypothesis. Since

$$\binom{Q!-1}{w} \quad \text{and} \quad \left(\frac{Q!}{w+1} - 1\right)$$

are coprime (Lemma 4.6) we have

$$a \equiv b \bmod\binom{Q!-1}{w+1}. \qquad \square$$

Lemma 4.8. *If $p \mid v!$ and p is prime then $p \leqslant v$.*

Proof. Induction on v. $\square$

Out next theorem is a preliminary version of the Matijasevič–Robinson–Davis–Putnam theorem, and is the main ingredient in the proof that $IE_1 + E \vdash I\Delta_0 + \exp$. Let $p(y, z, \boldsymbol{x}, \boldsymbol{a}) = p_+ - p_-$ be a polynomial, where p_+ and p_- are both terms in our original language, $\mathscr{L}$. We show how to find an E_1 formula $A(y, \boldsymbol{a}, v)$ in the language $\mathscr{L}_{\exp}$ equivalent to

$$\forall z < y\ \exists \boldsymbol{x} < v\, p(y, z, \boldsymbol{x}, \boldsymbol{a}) = 0$$

in $IE_1(2^x)$. For simplicity we write $\boldsymbol{x}$ as x_1, x_2 and omit $\boldsymbol{a}$ from our notation, it being clear from the proof how to obtain the result in its full generality. Let Q be $2y + p_+(y, y, v, v) + p_-(y, y, v, v) + v + 3$, so $Q > 2y > 0$. (Clearly we can assume $y \neq 0$, for otherwise write $\forall z < y\ \exists \boldsymbol{x} < v\, p(y, z, \boldsymbol{x}, \boldsymbol{a}) = 0$ as $y = 0 \vee (y > 0 \wedge \forall z < y\ \exists \boldsymbol{x} < v\, p(y, z, \boldsymbol{x}, \boldsymbol{a}) = 0)$.)

Theorem 4.9. $IE_1(2^x) \vdash \forall y > 0\, \forall v$

$$\Big\{\forall z < y\ \exists x_1, x_2 < v\, p(y, z, x_1, x_2) = 0$$

$$\leftrightarrow \exists b_1, b_2 \leqslant y(v+y)Q!\Big[b_1 > v \wedge b_2 > v$$

$$\wedge \binom{b_1}{v} \equiv \binom{b_2}{v} \equiv p(y, Q!-1, b_1, b_2) \equiv 0 \bmod\binom{Q!-1}{y}\Big]\Big\}.$$

Proof. ($\leftarrow$) Suppose $b_1, b_2 > v$ and

$$\binom{b_1}{v} \equiv \binom{b_2}{v} \equiv p(y, Q!-1, b_1, b_2) \equiv 0 \bmod \binom{Q!-1}{y}.$$

Write Q_z for $(Q!/(z+1)-1)$ for each $z < y$. Then by 4.1,

$$\forall z < y \; Q_z \mid \binom{Q!-1}{y}$$

so

$$\forall z < y \left[v! \binom{b_i}{v} \equiv 0 \bmod Q_z \right] \quad (i = 1, 2).$$

If p_z is prime and $p_z \mid Q_z$, then by 4.5 there is $x_i < v$ such that

$$p_z \mid (b_i - x_i) \quad (i = 1, 2),$$

hence by 4.4 we have

$$0 \equiv p(y, Q!-1, b_1, b_2) \equiv p(y, z, x_1, x_2) \bmod p_z$$

and by 4.2, $p_z > Q > |p(y, z, x_1, x_2)|$ hence $p(y, z, x_1, x_2) = 0$.

($\rightarrow$) Assume $\forall z < y \; \exists x_1, x_2 < v \, p(y, z, x_1, x_2) = 0$. We show by induction on w that

$$\forall w \leqslant y \left\{ w > 0 \rightarrow \exists b_1, b_2 \leqslant t \left[\binom{b_1}{v} \equiv \binom{b_2}{v} \right.\right.$$

$$\left.\left. \equiv p(y, Q!-1, b_1, b_2) \equiv 0 \bmod \binom{Q!-1}{w} \wedge b_1 > v \wedge b_2 > v \right] \right\}$$

where t is the term $t(w) = w(v+w)Q!$.

If $w = 1$, then let $x_1, x_2 < v$ satisfy $p(y, 0, x_1, x_2) = 0$ and $v < b_1, b_2 < t$ satisfy

$$b_i \equiv x_i \bmod (Q!-1) \quad (i = 1, 2).$$

For example, we may take $b_i = v(Q!-1) + x_i$.

For the induction step, given $b_1, b_2 < t(w)$ satisfying the formula for $w \geqslant 1$, where $w < y$, let x_1, x_2 satisfy

$$x_1, x_2 < v \wedge p(y, w, x_1, x_2) = 0.$$

Let $s = \binom{Q!-1}{w}$ so by 4.6 we have

$$\forall z < w \; (Q_z \mid s) \wedge (Q_w, s) = 1.$$

Choose u_1, u_2, s.t. $u_1, u_2 < Q_w$ and

$$u_i s \equiv x_i - b_i \bmod Q_w \quad (i = 1, 2)$$

(such u_i exists since in [12] it is shown that $IE_1 \vdash \forall x, y, a \, [(x, y) = 1 \rightarrow \exists z \; (xz \equiv a \bmod y)]$.) Now put

$$b_i' = b_i + s u_i \quad (i = 1, 2).$$

We claim that

(i) $\forall z < w\ b_i' \equiv b_i \bmod Q_z$ $(i = 1, 2)$, and

(ii) $b_i' \equiv x_i \bmod Q_w$ $(i = 1, 2)$.

(i) holds because $s \equiv 0 \bmod Q_z$ for each $z < w$, and (ii) holds because $b_i' \equiv b_i + (x_i - b_i) \equiv x_i \bmod Q_w$. Moreover, for each i,

$$\begin{aligned} b_i' &\leqslant b_i + sQ_w \\ &\leqslant t(w) + \binom{Q! - 1}{w + 1} \\ &\leqslant w(v + w)Q! + (w + 1)Q! \\ &\leqslant (w + 1)\left\{(v + w)\frac{w}{w + 1} + 1\right\}Q! \\ &\leqslant (w + 1)(v + w + 1)Q!. \end{aligned}$$

Thus it is only necessary to show that

$$\binom{b_1'}{v} \equiv \binom{b_2'}{v} \equiv p(y, Q! - 1, b_1', b_2') \equiv 0 \bmod \binom{Q! - 1}{w + 1}.$$

By a simple induction on k we can show that

$$v!\binom{b}{v} \equiv 0 \bmod m \rightarrow v!\binom{b + k}{v} \equiv 0 \bmod m$$

for all k, m, hence for all $z < w$

$$v!\binom{b_i'}{v} \equiv 0 \bmod Q_z \quad (i = 1, 2).$$

But $(v!, Q_z) = 1$ by 4.8 and 4.2, so for all $z < w$

$$\binom{b_i'}{v} \equiv 0 \bmod Q_z \quad (i = 1, 2).$$

We also have for each $z < w$

$$\begin{aligned} p(y, Q! - 1, b_1', b_2') &\equiv p(y, Q! - 1, b_1 + sQ_w, b_2 + sQ_w) \\ &\equiv p(y, Q! - 1, b_1, b_2) \equiv 0 \bmod Q_z \end{aligned}$$

since $s \equiv 0 \bmod Q_z$.

By induction we can show that

$$\forall b\ \forall v < b \left(b \mid v!\binom{b}{v}\right),$$

so

$$Q_w \mid b_i' - x_i \mid v!\binom{b_i' - x_i}{v} \Bigg| v!\binom{b_i'}{v}$$

hence

$$v!\binom{b_i'}{v} \equiv 0 \bmod Q_w \quad (i = 1, 2).$$

$(v!, Qw) = 1$, so

$$\binom{b_i'}{v} \equiv 0 \bmod Q_w \quad (i = 1, 2)$$

and as $Q! - 1 \equiv w \bmod Q_w$ by 4.4

$$p(y, Q! - 1, b_1', b_2') \equiv p(y, w, x_1, x_2) \bmod Q_w.$$

Thus using 4.7 we have

$$\binom{b_1'}{v} \equiv \binom{b_2'}{v} \equiv p(y, Q! - 1, b_1', b_2') \equiv 0 \bmod \binom{Q! - 1}{w + 1}$$

as required, completing the induction step and the proof. □

We now use 4.9 to prove the main result of this section:

Theorem 4.10. $IE_1 + E \vdash I\Delta_0 + \exp$.

Proof. Since $I\Delta_0 + \exp$ is a theory in the original language $\mathscr{L}$, by 3.4 it is sufficient to show $IE_1(2^x) \vdash I\Delta_0 + \exp$. We shall first show that for all $n \geqslant 1$ $IE_1(2^x) \vdash IE_n$, by induction on n.

If $IE_1(2^x) \vdash IE_n$, then by 3.4 again it is sufficient to show $IE_n(2^x) \vdash IE_{n+1}$. Let $\theta(z, \boldsymbol{a})$ be E_{n+1}, and suppose it is of the form

$$\exists z_1 < t_1(x, \boldsymbol{a})\, \forall z_2 < t_2(x, \boldsymbol{a}) \cdots Q z_{n-1} < t_{n-1}(x, \boldsymbol{a})\, \psi(x, \boldsymbol{a}, \boldsymbol{z})$$

where $Q = \exists$ or $\forall$ and ψ is U_2 or E_2 if n is even or odd respectively. Using the pairing function $\langle x, y \rangle = (x + y + 1)^2 + x$ we may assume that ψ (or $\neg\psi$) is of the form

$$\forall y < v\, \exists w < s\, p(y, v, w, s, x, a, z) = 0$$

by 1.4. 4.9 then shows how ψ (or $\neg\psi$) may be made equivalent to an E_1 formula in the extended language $\mathscr{L}_{\exp}$. Thus θ itself is equivalent to an E_n formula in $\mathscr{L}_{\exp}$ and we may use the induction scheme $IE_n(2^x)$ to show that the axiom of induction for θ holds.

Finally, to show that $IE_1 + E \vdash \exp$, let $\eta(x, y, z)$ be the Δ_0 formula representing the graph of exponentiation described in Section 1, and suppose n is sufficiently large so that IE_n proves η has the properties there and $\eta \in E_n$. Then in $IE_n(2^x)$ we can show by induction on y for any fixed parameter x that

$$\forall y\, \exists z \leqslant 2^{xy}\, \eta(x, y, z)$$

and hence $IE_1 + E \vdash \exp$. □

Corollary 4.11. *For all* $\theta(\boldsymbol{x}) \in \Sigma_1$ *there is* $\psi(\boldsymbol{x}) \in \exists_1$ *such that*

$$IE_1 + E \vdash \forall \boldsymbol{x}\, (\theta(\boldsymbol{x}) \leftrightarrow \psi(\boldsymbol{x}))$$

and

$$I\exists_1 \vdash \forall \boldsymbol{x}\, (\theta(\boldsymbol{x}) \leftrightarrow \psi(\boldsymbol{x})).$$

Proof. This is the statement of Matijasevič's Theorem true in $I\Delta_0 + \exp$, but as $I\exists_1 \vdash E$ and by 4.10, it also holds in the theories $I\exists_1$ and $IE_1 + E$. □

5. Parameter-free diophantine induction

Historically, the most difficult part of the solution of Hilbert's tenth problem was to show that there is a diophantine equation representing the graph of a function of exponential growth. This was Matijasevič's contribution in 1970, and was proved in $I\Delta_0 + \exp$ by Gaifman and Dimitracopoulos in [3]. We have managed to avoid this step altogether (except for an appeal to Gaifman and Dimitracopoulos's work) by means of the function $Y_a(x)$ and making very heavy use of the parameters in the induction scheme IE_1 throughout Sections 2, 3 and 4, and especially implicitly in the several uses of Theorems 2.7 and 3.4. One may suppose then that this use of parameters is actually necessary and neither $IE_1^- + E$ nor $I\exists_1^-$ can prove Matijasevič's Theorem. Surprisingly this turns out not to be true, and both these theories do prove Matijasevič's Theorem by essentially the same proof as we have given above. Our aim in this section is to show why. Along the way we will prove an interesting result about axiomatizations of theories that can prove Matijasevič's Theorem.

Definition. If Γ is a class of formulas then $J\Gamma$ is the theory PA^- together with

$$\forall x, \boldsymbol{a}\, (\theta(x, \boldsymbol{a}) \rightarrow \theta(x+1, \boldsymbol{a})) \rightarrow \forall x, \boldsymbol{a}\, (\theta(0, \boldsymbol{a}) \rightarrow \theta(x, \boldsymbol{a}))$$

for all $\theta \in \Gamma$.

It is clear that $I\Gamma \vdash J\Gamma \vdash I\Gamma^-$. We aim to show that if $\Gamma = E_n$, $\exists_n$ or Σ_n for $n \geqslant 1$ then $I\Gamma^- \vdash J\Gamma$.

Lemma 5.1. $IE_1^- \vdash$

(i) $\forall a\, \exists b\, 2b = a(a+1)$,

(ii) $\forall n\, \exists! a, b \leqslant n\, (n = a(a+1)/2 + b \wedge b \leqslant a)$.

Proof. (i) is easy. For (ii), to show existence we use induction on n. For $n = 0$ put $a = b = 0$. If

$$n = \frac{a(a+1)}{2} + b \wedge b < a \leqslant n$$

then $n+1=a(a+1)/2+(b+1)$ and we are done. If $a=b\leqslant n$ and $n=a(a+1)/2+b$, notice that

$$\frac{a(a+1)}{2}+(a+1)=\frac{(a+1)(a+2)}{2}\wedge a+1\leqslant n+1.$$

To show uniqueness, suppose

$$\frac{a(a+1)}{2}+b=\frac{a'(a'+1)}{2}+b'$$

with $b'\geqslant b$, $b\leqslant a$ and $b'\leqslant a'$. Then

$$\frac{a'(a'+1)}{2}\leqslant\frac{a'(a'+1)}{2}+(b'-b)=\frac{a(a+1)}{2}<\frac{(a'+1)(a'+2)}{2}$$

since $0\leqslant b'-b<a'+1$. Hence

$$a'\leqslant a<a'+1$$

and so $a=a'$ and $b=b'$ as required. □

Let $\langle x,y\rangle=z$ be the formula

$$(x>y\wedge z=x^2+y)\vee(x\leqslant y\wedge z=y^2+y+x)$$

This will serve as a pairing function. (We can't use $(x+y+1)^2+x$ at this stage since we don't know (yet!) that $IE_1^-\vdash IOpen$.)

Lemma 5.2. $IE_1^-\vdash$

(i) $\forall x,y\,\exists!z,\langle x,y\rangle=z$,

(ii) $\forall z\,\exists!x\,\exists!y\,\langle x,y\rangle=z$,

(iii) $\forall x,y,z\,(\langle x,y\rangle=z\rightarrow z\geqslant x\wedge z\geqslant y)$.

Proof. (i) and (iii) are trivial. $\forall z\,\exists x,y\leqslant z\,(\langle x,y\rangle=z)$ is by induction on z. If $z=0$ then put $x=y=0$. If $z=x^2+y\wedge x>y$ then either $z+1=x^2+(y+1)$ and $x>y+1$ or $y+1=x$ and $z+1=(y+1)^2+(y+1)+0$. If $z=y^2+y+x$ and $x\leqslant y$ then either $z+1=y^2+y+(x+1)$ and $x+1\leqslant y$ or $x=y$ and $z+1=x^2+x+x+1=(x+1)^2+0$.

Finally, uniqueness: if $z=x^2+y=x'^2+y'$ with $x>y$ and $x'>y'$ then

$$x^2\leqslant z<(x+1)^2\wedge x'^2\leqslant z<(x'+1)^2$$

so $x=x'$ and $y=y'$. The case $z=y^2+y+x=y'^2+y'+x'$ with $y\geqslant x$ and $y'\geqslant x'$ is similar. If $z=x^2+y=y'^2+y'+x'$ with $x>y$ and $y'\geqslant x'$ then $x=y'$ (by the same argument) and hence

$$y=z-x^2=z-y'^2=y'+x$$

so $y\geqslant x$, a contradiction. □

Lemma 5.3. *For $n \geq 1$ let Γ be E_n, $\exists_n$, or Σ_n. Then for all $\theta(x, \boldsymbol{a}) \in \Gamma$,*

$$I\Gamma^- \vdash (\forall \boldsymbol{a}\, \theta(0, \boldsymbol{a}) \wedge \forall \boldsymbol{a}, x\, (\theta(x, \boldsymbol{a}) \rightarrow \theta(x+1, \boldsymbol{a}))) \rightarrow \forall \boldsymbol{a}, x\, \theta(x, \boldsymbol{a}).$$

Proof. Using the pairing function $\langle x, y \rangle$ of Lemma 5.2 we may assume $\boldsymbol{a}$ is a single variable a. Let $\psi(n)$ be the formula

$$\exists a, b, c, d \leq n \left[n = \frac{d(d+1)}{2} + b \wedge b \leq d \wedge \langle a, c \rangle = d \wedge \theta(b, a) \right].$$

Suppose also $\forall a\, \theta(0, a) \wedge \forall a, x\, (\theta(x, a) \rightarrow \theta(x+1, a))$. We show that $\psi(0) \wedge \forall n\, (\psi(n) \rightarrow \psi(n+1))$.

If $n = d(d+1)/2$ (this includes the case $n = 0$) then by 3.2 $d = \langle a, c \rangle$ for some $a, c \leq d$, and $\psi(n)$ is equivalent to $\theta(0, a)$ which is true by our assumption.

Otherwise $n = d(d+1)/2 + b$ for some d, b with $b \leq d$. Suppose $\psi(n)$ holds. We must show that $\psi(n+1)$ holds. We may assume $b < d$ (for otherwise $n+1 = (d+1)(d+2)/2$ and we are back in the first case.) Let $d = \langle a, c \rangle$. Then $\psi(n)$ tells us that $\theta(b, a)$ holds, but as $b < d$, $n+1 = d(d+1)/2 + (b+1)$, with $b+1 \leq d$ and by assumption $\theta(b+1, a)$ is true, $\psi(n+1)$, as required. By $I\Gamma^-$ we deduce that $\forall n\, \psi(n)$.

Now given any x, a, put $c = x$, $d = \langle a, c \rangle$ and $n = d(d+1)/2 + x$, so $x \leq d$ and from $\psi(n)$ we deduce that $\theta(x, a)$ and the proof is complete. □

Theorem 5.4. *For $n \geq 1$ and $\Gamma = E_n$, $\exists_n$ or Σ_n we have*

$$I\Gamma^- \vdash J\Gamma.$$

Proof. Assume $\theta \in \Gamma$ and

$$\forall \boldsymbol{a}, x\, (\theta(x, \boldsymbol{a}) \rightarrow \theta(x+1, \boldsymbol{a})).$$

Suppose θ is $\exists z\, \psi(x, \boldsymbol{a}, z)$ where ψ and $\neg\psi$ are both in Γ (e.g. let ψ be the result of removing the first block of quantifiers from θ). Consider the formula $\phi(x, \boldsymbol{a}, z)$ in Γ, which is

$$\theta(x, \boldsymbol{a}) \vee \neg\psi(0, \boldsymbol{a}, z).$$

Then $\forall \boldsymbol{a}, z\, \phi(0, \boldsymbol{a}, z)$, for either $\psi(0, \boldsymbol{a}, z)$ hence $\theta(0, \boldsymbol{a})$, or $\neg\psi(0, \boldsymbol{a}, z)$ is true. Also,

$$\forall x, \boldsymbol{a}, z\, (\phi(x, \boldsymbol{a}, z) \rightarrow \phi(x+1, \boldsymbol{a}, z))$$

since if $\phi(x, \boldsymbol{a}, z)$ then either $\theta(x, \boldsymbol{a})$ and hence $\theta(x+1, \boldsymbol{a})$, or $\neg\psi(0, \boldsymbol{a}, z)$. By 5.3 we have in $I\Gamma^-$,

$$\forall x, \boldsymbol{a}, z\, (\theta(x, \boldsymbol{a}) \vee \neg\psi(0, \boldsymbol{a}, z))$$

so $\forall x, \boldsymbol{a}\, (\theta(0, \boldsymbol{a}) \rightarrow \theta(x, \boldsymbol{a}))$ as required. □

Let $n \geq 1$ and $\Gamma = E_n$, $\exists_n$ or Σ_n as before. A sentence σ is $\forall\Gamma$ if it is $\forall \boldsymbol{x}\, \gamma(\boldsymbol{x})$ for

some $\gamma \in \Gamma$, and σ is $\exists\forall\Gamma$ if it is $\exists \boldsymbol{x}\, \forall \boldsymbol{y}\, \gamma(\boldsymbol{x}, \boldsymbol{y})$ for some $\gamma \in \Gamma$. We can now use 5.4 to prove the following conservation result:

Theorem 5.5. *For Γ as above, if $\sigma \in \exists\forall\Gamma$ and $I\Gamma \vdash \sigma$ then $I\Gamma^- \vdash \sigma$.*

Proof. Suppose $M \models I\Gamma^- + \tau$ where τ is $\forall \boldsymbol{x}\, \exists \boldsymbol{y}\, \gamma(\boldsymbol{x}, \boldsymbol{y})$ and $\neg\gamma \in \Gamma$. It is required to show that there is a model of $I\Gamma + \tau$. Using the pairing function $\langle , \rangle$ we may assume $\boldsymbol{x}$ and $\boldsymbol{y}$ are both single variables x, y.

We use a Henkin-style argument to construct our model. We shall construct a sequence $\phi_0(x_0, \ldots, x_{i_0}), \ldots, \phi_j(x_0, \ldots, x_{i_j}), \ldots$ of formulas in $\neg\Gamma$ ($= U_n$, $\forall_n$ or Π_n) with $\vdash \phi_{i+1}(\boldsymbol{x}) \rightarrow \phi_i(\boldsymbol{x})$ for each i, and satisfying (i)–(vi).

(i) $M \models \exists \boldsymbol{x}\, \phi_i(\boldsymbol{x})$, each i.

(ii) For all $j \in \mathbb{N}$ there is $k \in \mathbb{N}$ and $l \leqslant i_k$ such that

$$\vdash \phi_k(\boldsymbol{x}) \rightarrow \gamma(x_j, x_l);$$

(iii) For each $\psi \in \neg\Gamma$ and each k, if

$$M \models \forall \boldsymbol{x}\, (\phi_k(\boldsymbol{x}) \rightarrow \exists \boldsymbol{y}\, \psi(\boldsymbol{x}, \boldsymbol{y}))$$

then for some j and for some $\boldsymbol{z}$ from $x_0, x_1, \ldots,$

$$\vdash \phi_j \rightarrow \psi(\boldsymbol{x}, \boldsymbol{z});$$

(iv) For each $\psi(z)$ in $\forall\Gamma$ with $\boldsymbol{z}$ from $x_0, x_1, \ldots,$ there is $j \in \mathbb{N}$ such that

either: $M \models \forall \boldsymbol{x}\, (\phi_j \rightarrow \psi(\boldsymbol{z}))$

or: $M \models \forall \boldsymbol{x}\, (\phi_j \rightarrow \neg\psi(\boldsymbol{z}))$;

(v) For each axiom $\forall \boldsymbol{a}\, \exists \boldsymbol{b}\, \psi(\boldsymbol{a}, \boldsymbol{b})$ of PA^- (where ψ is quantifier free) and each $\boldsymbol{y}$ from $x_0, x_1, \ldots$ there is $k \in \mathbb{N}$ and $\boldsymbol{z}$ from $x_0, x_1, \ldots$ such that

$$\vdash \phi_k \rightarrow \psi(\boldsymbol{y}, \boldsymbol{z});$$

(vi) For each $\theta(x, \boldsymbol{y}) \in \Gamma$ and each $\boldsymbol{y}$ from $x_0, x_1, \ldots$ we have,

either: for all x_i there is j such that

$$\vdash \phi_j(\boldsymbol{x}) \rightarrow \theta(x_i, \boldsymbol{y}),$$

or: for some x_i and some j we have

$$\vdash \phi_j(\boldsymbol{x}) \rightarrow (\neg\theta(0, \boldsymbol{y}) \vee (\theta(x_i, \boldsymbol{y}) \wedge \neg\theta(x_i + 1, \boldsymbol{y}))).$$

To satisfy (ii) subject to (i) suppose we have constructed ϕ_i and are considering x_j. Then $M \models \exists \boldsymbol{x}\, \phi_i(\boldsymbol{x}) \wedge \forall y\, \exists z\, \gamma(y, z)$ hence for any new variable x_l put $\phi_{i+1}(\boldsymbol{x}, x_l) \stackrel{\text{def}}{=} \phi_i(\boldsymbol{x}) \wedge \gamma(x_j, x_l)$ so $M \models \exists \boldsymbol{x}, x_l\, \phi_{i+1}(\boldsymbol{x}, x_l)$. (v) is exactly the same. Conditions (iii) and (iv) are the standard Henkin conditions and it is left to the reader to check that these can always be satisfied. This leaves (vi).

If any any stage $\phi_j(\boldsymbol{x})$ of the construction we have

$$M \models \exists \boldsymbol{x}, z\, (\phi_j(\boldsymbol{x}) \wedge \neg\theta(z, \boldsymbol{y}))$$

where $\boldsymbol{y}$ are amongst the $x_0, x_1, \ldots$, and z is a new variable, then either

$$M \models \exists \boldsymbol{x}\, (\phi_j(\boldsymbol{x}) \wedge \neg\theta(0, \boldsymbol{y}))$$

or

$$M \models \exists \boldsymbol{x}, z\, ((\neg\phi_j(\boldsymbol{x}) \vee \theta(z, \boldsymbol{y})) \wedge (\phi_j(\boldsymbol{x}) \wedge \neg\theta(z+1, \boldsymbol{x})))$$

using $J\Gamma$ on $\neg\phi_j(\boldsymbol{x}) \vee \theta(z, \boldsymbol{y})$ in M. Hence

$$M \models \exists \boldsymbol{x}, z\, (\phi_j \wedge (\neg\theta(0, \boldsymbol{y}) \vee (\theta(z, \boldsymbol{y}) \wedge \neg\theta(z+1, \boldsymbol{y})))).$$

If $\theta(z, \boldsymbol{y})$ is $\exists \boldsymbol{u}\, \psi(z, \boldsymbol{y}, \boldsymbol{u})$ where $\psi \in \neg\Gamma$ we can just put ϕ_{j+1} to be

$$\phi_j \wedge (\neg\theta(0, \boldsymbol{y}) \vee (\psi(x_i, \boldsymbol{y}, x_{i+1}, \ldots, x_{i+k}) \wedge \neg\theta(x_i + 1, \boldsymbol{y})))$$

for new variables $x_i, x_{i+1}, \ldots, x_{i+k}$ not already occurring in ϕ_j.

Otherwise, when considering $\boldsymbol{y}$ at stage ϕ_k, we may always suppose that

$$M \models \forall \boldsymbol{x}, z\, (\phi_k \rightarrow \theta(z, \boldsymbol{y}))$$

so we may just put $\phi_{k+1}(\boldsymbol{x}, x_i)$ equal to

$$\phi_j(\boldsymbol{x}) \wedge \psi(x_i, \boldsymbol{y}, \boldsymbol{w})$$

for some new constants $\boldsymbol{w}$ from $x_0, x_1, \ldots$.

Having constructed the ϕ_i, the rest of the proof is standard. Let $\langle M', c_0, c_1, \ldots\rangle$ be a model of $\mathrm{Th}(M) + \{\phi_i(c_0, c_1, \ldots) \mid i \in \mathbb{N}\}$ and consider the substructure K of M' consisting of all the c_i's. Then $K \prec_{\forall\Gamma} M'$ by (iii) and (iv), $K \models \tau$ by (ii), $K \models PA^-$ by (v), and $K \models I\Gamma$ by (vi). Thus $I\Gamma \not\vdash \neg\tau$ as required. □

For proof-theorists. An alternative proof of Theorem 5.5 using the cut-elimination theorem can be obtained in the following way. Supposing that $\neg\sigma$ is $\forall \boldsymbol{x}\, \exists y_1, \ldots, y_k\, \gamma(\boldsymbol{x}, y_1, \ldots, y_k)$ with $\neg\gamma \in \Gamma$ and $I\Gamma \vdash \sigma$, we expand our language to $\mathscr{L}^+$ which has Skolem functions $S_1(\boldsymbol{x}), \ldots, S_k(\boldsymbol{x})$ for $\neg\sigma$. Then $I\Gamma + \forall \boldsymbol{x}\, \gamma(\boldsymbol{x}, S_1(\boldsymbol{x}), \ldots, S_k(\boldsymbol{x}))$ is inconsistent. We may formalize this theory using a Gentzen-style sequent calculus with the usual rules together with the induction rule

$$\frac{\Xi,\ \theta(\boldsymbol{t}, x) \vdash \theta(\boldsymbol{t}, x+1),\ \Lambda}{\Xi,\ \theta(\boldsymbol{t}, 0) \vdash \theta(\boldsymbol{t}, s),\ \Lambda}$$

(where $\boldsymbol{t}$, s are terms in $\mathscr{L}^+$, θ is a formula in Γ and the variable x does not appear free in either Ξ or Λ) together with axioms

$$\Xi \vdash \gamma(\boldsymbol{t}, S_1(\boldsymbol{t}), \ldots, S_k(\boldsymbol{t})),\ \Lambda \quad \text{and} \quad \Xi, \neg\gamma(\boldsymbol{t}, S_1(\boldsymbol{t}), \ldots, S_k(\boldsymbol{t})) \vdash \Lambda$$

for any Ξ, Λ and $\mathscr{L}^+$-terms $\boldsymbol{t}$. Since the resulting system is inconsistent, cut-elimination shows that there is a proof of an inconsistency which only involves formulas which are either in Γ or have negations in Γ. By rearranging we may assume that all formulas are in Γ. Now by induction on the length of this proof we have

$$I\Gamma^- + \forall \boldsymbol{x}\, \gamma(\boldsymbol{x}, \boldsymbol{S}(\boldsymbol{x})) \vdash \forall \boldsymbol{x}\, (\bigwedge \Xi(\boldsymbol{x}) \rightarrow \bigvee \Lambda(\boldsymbol{x}))$$

for all sequents $\Xi(\boldsymbol{x}) \vdash \Lambda(\boldsymbol{x})$ occurring in the proof. (The only difficult step here is the one for the induction rule: this requires Lemma 5.4.) Thus $I\Gamma^- + \neg\sigma$ is also inconsistent, and so $I\Gamma^- \vdash \sigma$, as required. (Essentially the model-theoretic proof of 5.5 above is a Henkin-style proof of the completeness theorem for the relevant 'cut-free' proof-system above.)

Corollary 5.6. *For each* $n \geq 1$

(i) $IE_n^- \vdash IU_n^- + IE_{n-1}$,
(ii) $I\exists_n^- \vdash I\forall_n^- + I\exists_{n-1}$,
(iii) $I\Sigma_n^- \vdash I\Pi_n^- + I\Sigma_{n-1}$,
(iv) $I\Delta_0^- \vdash I\Delta_0$.

Proof. Clearly $IE_n \vdash IU_n^- + IE_{n-1}$, IU_n^- is $\exists\forall E_{n-1}$ axiomatizable and IE_{n-1} is $\forall E_n$ axiomatizable. (ii)–(iv) are proved similarly. □

Remark. Direct proofs of (iii) and (iv) can be found in [4].

We now return to considering Matijasevič's Theorem:

Theorem 5.7. *Suppose* T *is a theory with a* Π_n *axiomatization for some* $n \geq 2$, *and* $T \vdash$ *Matijasevič's Theorem. Then* T *has an* $\forall_n$ *axiomatization.*

Proof. We show by induction on formulas that for all $\theta \in \Sigma_1$ there is $\sigma_\theta \in \forall_2$ and $\psi_\theta \in \exists_1$ such that

$$T \vdash \sigma_\theta \vdash \forall \boldsymbol{x}\, (\theta(\boldsymbol{x}) \leftrightarrow \psi_\theta(\boldsymbol{x})).$$

If $\theta \in \exists_1$ the result is trivial, and if θ is $\exists y\, \theta_1(\boldsymbol{x}, y)$, $\theta_1 \vee \theta_2$ or $\theta_1 \wedge \theta_2$ then the induction step is easy. The only remaining case is when θ is $\neg\theta_1$ for some $\theta \in \Delta_0$. By the induction hypothesis there are σ_{θ_1}, ψ_{θ_1} in $\forall_2$, $\exists_1$ respectively, such that

$$T \vdash \sigma_{\theta_1} \vdash \forall \boldsymbol{x}\, (\theta_1(\boldsymbol{x}) \leftrightarrow \psi_{\theta_1}(\boldsymbol{x})).$$

Let ψ_θ satisfy

$$T \vdash \forall \boldsymbol{x}\, (\theta(\boldsymbol{x}) \leftrightarrow \psi_\theta(\boldsymbol{x})).$$

with $\psi_\theta \in \exists_1$ by Matijasevič's Theorem in T. Let σ_1 be $\forall \boldsymbol{x}\, (\neg\psi_{\theta_1}(\boldsymbol{x}) \rightarrow \psi_\theta(\boldsymbol{x}))$ and let σ_2 be $\forall \boldsymbol{x}\, (\psi_\theta(\boldsymbol{x}) \rightarrow \neg\psi_{\theta_1}(\boldsymbol{x}))$, so σ_1 is $\forall_2$ and σ_2 is $\forall_1$. Finally, let σ_θ be

$$\sigma_{\theta_1} \wedge \sigma_1 \wedge \sigma_2$$

so

$$T \vdash \sigma_{\theta_1} \wedge \sigma_1 \wedge \sigma_2 \vdash \forall \boldsymbol{x}\, (\theta(\boldsymbol{x}) \leftrightarrow \psi_\theta(\boldsymbol{x})).$$

Now in the Π_n axiomatization of T, replace each axiom

$$\forall \boldsymbol{x}_1\, \exists \boldsymbol{x}_2 \cdots Q\boldsymbol{x}_n\, \theta(\boldsymbol{x})$$

(where $\theta \in \Delta_0$) by $\sigma_\theta \wedge \forall \boldsymbol{x}_1\, \exists \boldsymbol{x}_2 \cdots Q\boldsymbol{x}_n\, \psi_\theta(\boldsymbol{x})$ if n is even, and by $\sigma_{\neg\theta} \wedge \forall \boldsymbol{x}_1\, \exists \boldsymbol{x}_2 \cdots Q\boldsymbol{x}_n\, \neg\psi_{\neg\theta}(\boldsymbol{x})$ if n is odd. □

Remark. (i) Theorem 5.7 was first proved by Handley and Paris (unpublished) for the case $T = I\Delta_0 + \exp$ using the Łos–Susko theorem on unions of chains of models.

(ii) Z. Adamowicz has pointed out to the author that the conditions on T in 5.7 may be weakened to:

"For every $\theta \in \Delta_0$ such that θ or $\neg\theta$ occurs as a subformula of an axiom of T, there is some $\psi_\theta \in \exists_1$ such that, $T \vdash \forall \boldsymbol{x}\, (\theta(\boldsymbol{x}) \leftrightarrow \psi_\theta(\boldsymbol{x}))$."

(iii) Using Parikh's theorem (1.3) we may extend 5.7 as follows:

If T is a Π_1 theory in $\mathscr{L}$ that proves Matijasevič's Theorem (it is not known if any such T exists!) then T has an $\forall E_1$ axiomatization.

In particular, if IE_1 proves Matijasevič's Theorem then IE_1 is $\forall E_1$ and so by 5.5, is equivalent to $I\overline{E_1}$.

The next lemma is the analogue of Parikh's theorem for $IE_1 + E$. Let $\psi(a, b, x, y)$ be

$$p(a, x, y) = 0 \wedge x \leqslant y \wedge x \equiv b \bmod(a-1) \wedge y \equiv b+1 \bmod(a-1)$$

as in Section 2 and let $\chi(a, b)$ *be*

$$\exists c \leqslant b\ \psi(a+2, a, c, b).$$

Lemma 5.8. (i) *If* $IE_1 + E \vdash \forall \boldsymbol{x}\, \exists \boldsymbol{y}\, \theta(\boldsymbol{x}, \boldsymbol{y})$ *with* $\theta \in \Delta_0$, *then for some* $n \in \mathbb{N}$

$$IE_1 \vdash \forall \boldsymbol{x}, z_0, z_1, \ldots, z_n \left[z_0 = \max(\boldsymbol{x}) \wedge \bigwedge_{i=0}^{n-1} \chi(z_i, z_{i+1}) \rightarrow \exists \boldsymbol{y} \leqslant z_n\, \theta(\boldsymbol{x}, \boldsymbol{y}) \right].$$

(ii) *If* $IE_1 + E \vdash \forall \boldsymbol{x}\, \theta(\boldsymbol{x})$ *with* $\theta \in \Delta_0$, *then for some* $n \in \mathbb{N}$

$$IE_1 \vdash \forall \boldsymbol{x}, z_0, z_1, \ldots, z_n \left[z_0 = \max(\boldsymbol{x}) \wedge \bigwedge_{i=0}^{n-1} \chi(z_i, z_{i+1}) \rightarrow \theta(\boldsymbol{x}) \right].$$

Proof. (ii) is a special case of (i). We prove (i):

Notice first that, for each $n \in \mathbb{N}$,

$$IE_1 \vdash \forall a, b, c, d\, [(a \geqslant 2 \wedge b \geqslant n \wedge b \leqslant a-2 \wedge \psi(a, b, c, d)) \rightarrow d \geqslant a^n] \qquad (\ddagger)$$

(We leave this as an exercise for the reader using Lemma 2.1.) This means that if $M \models IE_1$ and $\mathbb{N} \subseteq_e I \subseteq_e M$ with

$$\forall x \in I\, \exists y \in I\, M \models \chi(x, y) \qquad (\S)$$

then I is an $\mathscr{L}$-structure (i.e. is closed under $+$, $\cdot$) so $I \models IE_1$ and also, by 2.6, we have $I \models E$.

Now suppose the conclusion of (i) is false for all $n \in \mathbb{N}$. By compactness there exists a model $M \models IE_1$ with $\boldsymbol{a}, \boldsymbol{b} \in M$ satisfying

$$M \models b_0 = \max(\boldsymbol{a}) \wedge \chi(b_i, b_{i+1}) \wedge \forall y \leqslant b_i\, \neg\theta(\boldsymbol{a}, \boldsymbol{y})$$

for each $i \in \mathbb{N}$.

Let $I \subseteq_e M$ be the initial segment of M defined by the b_i, i.e.

$$I = \{x \in M \mid \exists i \in \mathbb{N}\, M \models x \leqslant b_i\}$$

Then by 2.6 I satisfies (§) and hence is an $\mathscr{L}$-structure with $I \models IE_1 + E$. But clearly $\boldsymbol{a} \in I$ and since $M \models \forall \boldsymbol{y} \leqslant b_i \neg\theta(\boldsymbol{a}, \boldsymbol{y})$ for each i and this formula is Δ_0, by 1.4 we have $I \models \forall \boldsymbol{y} \neg\theta(\boldsymbol{a}, \boldsymbol{y})$, thus $IE_1 + E \not\vdash \forall \boldsymbol{x}\, \exists \boldsymbol{y}\, \theta(\boldsymbol{x}, \boldsymbol{y})$, as required. □

Corollary 5.9. (i) $IE_1^- + E \vdash I\Delta_0 + \exp$.

(ii) $I\exists_1^- \vdash I\Delta_0 + \exp$.

(iii) *Both* $IE_1^- + E$ *and* $I\exists_1^-$ *prove Matijasevič's Theorem.*

Proof. (i) Let $\sigma = \forall \boldsymbol{x}\, \exists \boldsymbol{y}\, \theta(\boldsymbol{x}, \boldsymbol{y})$ be any axiom of the $\forall\exists$ axiomatization of $I\Delta_0 + \exp$ given in 5.7. Then by 4.10,

$$IE_1 + E \vdash \sigma$$

so by 5.8, for some n,

$$IE_1 \vdash \forall \boldsymbol{x}, z \left[z_0 = \max(\boldsymbol{x}) \wedge \bigwedge_{i=0}^{n-1} \chi(z_i, z_{i+1}) \rightarrow \exists \boldsymbol{y} \leqslant z_n\, \theta(\boldsymbol{x}, \boldsymbol{y}) \right]$$

so by 5.5,

$$IE_1^- \vdash \forall \boldsymbol{x}, z \left[z_0 = \max(\boldsymbol{x}) \wedge \bigwedge_{i=0}^{n-1} \chi(z_i, z_{i+1}) \rightarrow \exists \boldsymbol{y} \leqslant z_n\, \theta(\boldsymbol{x}, \boldsymbol{y}) \right]$$

and hence $IE_1^- + E \vdash \sigma$.

(ii) E is $\forall\exists$ and $I\exists_1 \vdash E$ hence by 5.5, $I\exists_1^- \vdash E$.

(iii) Obvious from (i), (ii) and the Gaifman–Dimitracopoulos result that $I\Delta_0 + \exp \vdash$ Matijasevič's Theorem. □

Remark. It is interesting to notice that our arguments do indeed show how to construct proofs of $I\Delta_0 + \exp$ from $I\exists_1^-$ or $IE_1^- + E$ (but these proofs are so long that it would be impractical to write them down!)

To see this consider an $\forall_2$ axiomatization Σ of $I\Delta_0 + \exp$. Such an axiomatization together with the necessary proofs that

$$I\Delta_0 + E \vdash \Sigma \vdash I\Delta_0 + E$$

are easily found by consideration of the proof of Theorem 5.7 and Dimitracopoulos and Gaifman's work in [3]. Now for each sentence $\forall \boldsymbol{x}\, \exists \boldsymbol{y}\, \psi(\boldsymbol{x}, \boldsymbol{y})$ of Σ (where ψ is quantifier-free) we must modify the given proof of $I\Delta_0 + E \vdash \forall \boldsymbol{x}\, \exists \boldsymbol{y} \psi\, (\boldsymbol{x}, \boldsymbol{y})$ to one from $IE_1^- + E$ or $I\exists_1^-$. Considering $I\exists_1^-$ for the moment, since $I\Delta_0 + E$ is Π_2-axiomatized the cut-elimination theorem supplies us with a proof of $\exists \boldsymbol{y}\, \psi(\boldsymbol{x}, \boldsymbol{y})$ from $I\Delta_0 + E$ that only involves Σ_1 and Π_1 formulas. Moreover each use of induction only involves induction up to some predetermined $\mathscr{L}$-term. Thus by the prototype version of Matijasevič's Theorem described in Sections 2–4 (and culminating in Theorem 4.9) we can replace each

Π_1 or Σ_1 formula in the proof obtained so far by equivalent $\forall_1$ or $\exists_1$ formulas (with extra parameters) where this equivalence is provable in $I\exists_1$. By the proof of 5.7 again, this equivalence can be expressed using $\forall_2$ sentences, and so each instance of this equivalence that is needed can (by the cut-elimination theorem again) be proved using $\forall_1$ and $\exists_1$ formulas only. Thus we can append the proofs of these instances in the appropriate way, and by replacing each $I\exists_1$ *or* $I\Delta_0$ induction step with the corresponding $J\exists_1$ induction step we obtain a proof of $\exists y\, \psi(x, y)$ in $I\exists_1^-$ as required.

The argument for $IE_1^- + E$ is similar: the extra feature is that one must find exponential bounds for each unbounded quantifier in the proofs considered in the last paragraph. This amounts to asking for a constructive proof of Lemma 5.8, and this can be obtained easily by modifying Parikh's original argument given in [8].

6. On the structure of models of bounded diophantine induction

In this section we shall examine some of the consequences of results from Sections 2–5 for the structure of nonstandard models of IE_1 and IE_1^-. It is known that a countable nonstandard model M of IE_1 is not recursive [12] and has a nonstandard initial segment satisfying Peano's axioms, *PA* [6]. We present new proofs of these facts based on our work above, giving a little more information, and then consider the analogous question for IE_1^-. It turns out that this latter question is closely related to the more general question: "What relations are represented by E_1 formulas (in $\mathbb{N}$)?".

Let $\psi(a, b, x, y)$ be

$$p(a, x, y) = 0 \wedge x \leqslant y \wedge x \equiv b \bmod(a-1) \wedge y \equiv b+1 \bmod(a-1)$$

and let $\chi(a, b)$ be $\exists c \leqslant b\, \psi(a+2, a, c, b)$ as in Section 5. We shall use 2.4, 2.6 and the sentence (‡) in the proof of 5.8 often. Notice that each of these say IE_1 proves a certain $\forall E_1$ sentence. Thus by 5.5 we may apply these results to IE_1^- also.

For any model M of IE_1^- we let

$$M_0 = M,$$
$$M_{i+1} = \{a \in M \mid \exists b \in M_i\, M \vDash \chi(a, b)\},$$
$$M_{\exp} = \bigcap_{i \in \mathbb{N}} M_i.$$

These M_i need not be structures for $\mathcal{L}$ (in fact they might even have a greatest element) but by 2.6 we can deduce that $M_{\exp} \subseteq_e \cdots \subseteq_e M_i \subseteq_e \cdots \subseteq_e M_2 \subseteq_e M_1 \subseteq_e M_0 = M$. Since χ is Δ_0, $\mathbb{N} \vDash \forall x\, \exists y\, \chi(x, y)$ and $\mathbb{N} \vDash \chi(n, m)$ iff $M \vDash \chi(n, m)$ for all $n, m \in \mathbb{N}$, we have also $\mathbb{N} \subseteq_e M_{\exp}$.

We shall in fact show that $M_{\exp} \vDash I\Delta_0 + \exp$, and is the largest cut in M satisfying E.

Lemma 6.1. $IE_1 \vdash \forall x \geq 1\ \exists y, z \leq x\ (\chi(y, z) \wedge \forall w \leq x\ \neg\chi(y+1, w))$.

Proof. If not, there is a $a \in M \models IE_1$ with $a \geq 1$ and

$$M \models \forall y < a\ (\exists z \leq a\ \chi(y, z) \rightarrow \exists z \leq a\ \chi(y+1, z)).$$

So since $M \models \chi(0, 1)$, by IE_1 induction on y we have $M \models \exists z \leq a\ \chi(a, z)$ which is absurd. □

Remark. We do not know if the sentence above is provable from IE_1^-. Notice it is $\forall E_2$, so we cannot apply 5.5. Denote this sentence by L ('L' for '*Log*', since it states the existence of a function of roughly logarithmic growth.)

Lemma 6.2. *If* $M \models IE_1^- + \neg E + L$ *then* $M_i \neq M_{i+1}$ *for each* $i \in \mathbb{N}$.

Proof. Clearly $M_i = M_{i+1}$ iff M_i is an $\mathscr{L}$-structure and $M_i \models E$. We show that $M_{i+1} \models E \Rightarrow M_i = M_{i+1}$ which therefore suffices. If $M_{i+1} \models E$ and $a \in M_i$ let $x, y \leq a$ satisfy $M \models \chi(x, y) \wedge \forall z \leq a\ \neg\chi(x+1, z)$. Then clearly $y \in M_i$ and $x \in M_{i+1}$. But if $M_{i+1} \models E$ then M_{i+1} is an $\mathscr{L}$-structure, so $x+1 \in M_{i+1}$ and $\exists z \in M_{i+1}\ M_{i+1} \models \chi(x+1, z)$. χ is Δ_0 and $M_{i+1} \subseteq_e M$ so $M \models \chi(x+1, z)$ hence $M \models a < z$ and so $a \in M_{i+1}$ as required. □

Proposition 6.3. *If* $M \models IE_1^-$ *is nonstandard and* $M_i \neq M_{i+1}$ *for all* $i \in \mathbb{N}$ *then*

(i) $M_{\exp} \models E$,

(ii) $M_{\exp} \neq \mathbb{N}$,

(iii) *there is a cut* I *with* $I \models I\Delta_0$, $I \neq M_{\exp}$ *and*

$$M_{\exp} \subseteq_e I,$$

hence $M_{\exp} \models I\Delta_0 + B\Sigma_1 + \exp$.

Proof. (For the definition of $B\Sigma_1$ see [7].)

Using truth definitions for E_n formulas, Paris and Dimitracopoulos (see e.g. [2]) have shown that for all n there is a Π_1 sentence σ_n such that

$$I\Delta_0 \vdash \sigma_n \vdash IE_n.$$

Let σ_n be $\forall x\ \phi_n(x)$ with $\phi_n \in \Delta_0$. If $a \in M$ let $a^{1/\mathbb{N}}$ denote the cut

$$a^{1/\mathbb{N}} \stackrel{\text{def}}{=} \{y \in M \mid \forall n \in \mathbb{N}\ M \models y^n < a\}$$

so that $a^{1/\mathbb{N}}$ is closed under both $+$ and $\cdot$. Since

$$IE_1^- + E \vdash I\Delta_0 \vdash \forall x\ \forall y \leq x\ \phi_n(y),$$

by 5.8 there is $i \in \mathbb{N}$ such that for all $a \in M_i$, $M \models \forall y \leq a\ \phi_n(y)$. If $a \in M_i - M_{i+1}$ then

$$M_{i+2} \subseteq_e a^{1/\mathbb{N}} \models IE_n.$$

(The inclusion $M_{i+2} \subseteq_e a^{1/\mathbb{N}}$ is from $M \models \forall b, c\, (\chi(b, c) \wedge c \leqslant a \rightarrow b^n \leqslant a)$ for all $n \in \mathbb{N}$ from (‡) in the proof of 5.8.)

Thus for all n there is $i \in \mathbb{N}$ and a cut I with $M_{i+2} \subseteq_e I \subseteq_e M_i$ and $I \models IE_n$. To show (i) suppose $M_{i+2} \subseteq_e I \subseteq_e M_i$, $I \models IE_1$ and $a \in M_{\exp}$. Then for all $j \leqslant i + 2$ there is $b \in M_j$ with $M \models \chi(a, b)$. Using IE_1 in I we have

$$I \models \exists b\, \chi(a, b) \wedge \forall z < b\, \neg\chi(a, z)$$

hence it follows that this particular b must be in all the M_j, i.e. $b \in M_{\exp}$.

To show (ii), let

$$g(x) = y \overset{\text{def}}{\iff} \exists c \leqslant x\, (\chi(y, c) \wedge \forall w \leqslant x\, \neg\chi(y + 1, w))$$

and

$$f(x) = \begin{cases} 0 & \text{if } x = 0, \\ 1 + f(g(x)) & \text{otherwise.} \end{cases}$$

Then $f(x)$ has a Δ_0 graph and for some $n \in \mathbb{N}$

$$IE_n \vdash \forall x\, \exists! y\, f(x) = y \wedge \forall x, y\, (f(x) > f(y) \rightarrow x > y).$$

Let $I \supseteq_e M_{\exp}$ satisfy IE_n and let $a \in I - M_{\exp}$ and $b \in I$ satisfy

$$I \models f(a) = b.$$

Then clearly $b \in M_{\exp}$, since a is nonstandard. Also b is nonstandard, for $\mathbb{N} \models \forall x\, \exists y\, f(y) = x$ and if $c \in \mathbb{N}$ with $\mathbb{N} \models f(c) = b + 1$ then $I \models a < c$.

To show (iii) let $x \in y$ be the standard Δ_0 formula expressing "the xth digit in the binary expansion of y is 1", $|x|$ the standard Δ_0 function denoting the length of the binary expansion of x, and let $M_i \subseteq_e I \models IE_n$ with n sufficiently large to prove a (finite) set of basic properties of $+$, $\cdot$, $<$, $\in$ and $|\cdot|$ provable in $I\Delta_0$, including:

(1) $\forall a\, \exists s\, \forall x, y < \|a\|\, \forall z < 2\,\|a\|\, (\langle x, y, z\rangle \in s \leftrightarrow x + y = z)$

and similar sentences for $\cdot$, $<$, projection functions, and permutation and substitution of variables;

(2) $\forall a, b, s\, \exists t\, \forall x \leqslant b\, (x \in t \leftrightarrow \exists y < a\, \langle x, y\rangle \in s)$,

(3) $\forall a, b, s_1, s_2\, \exists t\, \forall x \leqslant a\, \forall y \leqslant b\, (\langle x, y\rangle \in t \leftrightarrow (x \in s_1 \wedge y \in s_2))$,

(4) $\forall a, s\, \exists t\, \forall x \leqslant |a|\, (x \in t \leftrightarrow \neg x \in s)$,

(5) $\forall s\, (\exists x\, (x \in s) \rightarrow \exists x\, (x \in s \wedge \forall y < x\, (y \notin s)))$.

Notice that (by a suitable choice of pairing function) each of these sentences are provable in $I\Delta_0$. It follows that if $a \in I - M_i$ and J is any cut in I with $J \neq M_{\exp}$ and $M_{\exp} \subseteq_e J < \|a\|$ (there are such cuts, since $\|a\| > M_{i+2}$) then for each Δ_0 formula $\theta(x)$ and for each $a \in J$ there is $s \in I$ with

$$I \models \forall x \leqslant a\, (\theta(x) \leftrightarrow x \in s).$$

It follows from (5) above that $J \models I\Delta_0$ as required.

It follows immediately from the fact that $M_{\exp}$ has a proper end extension $J \models I\Delta_0$ that $M_{\exp} \models B\Sigma_1$ by a result in [7]. □

Remark. My thanks to Jeff Paris for pointing out part (iii) of the above proposition to me.

Corollary 6.4. *If $M \models IE_1$ or $IE_1^- + L$ is nonstandard and countable, then*
(i) *M has a nonstandard initial segment $I \models PA$, and*
(ii) *neither $+^M$ nor $\cdot^M$ can be recursive.*

Proof. (i) By a result of McAloon [5], any nonstandard model of $I\Delta_0$ has a nonstandard initial segment $I \models PA$. If $M \models E$ then $M \models I\Delta_0 + \exp$ by 5.9 so we can apply this result directly. If $M \models \neg E$ then $\mathbb{N} \neq M_{\exp} \models I\Delta_0 + \exp$ so $M_{\exp}$ has a nonstandard initial segment $I \models PA$. (ii) follows from (i) by Tennenbaum's original argument, [11]. □

I do not known if we can extend this result to the case $M \models IE_1^- + \neg L$. The problem is that it appears to be possible that $M_0 \supseteq_e M_1 \supseteq_e \cdots \supseteq_e M_i = M_{i+1} = \cdots = M_{\exp} \supseteq_e \mathbb{N}$ for some i. Of course even in this case it is sufficient just to show $M_{\exp} \neq \mathbb{N}$. A partial result along these lines follows:

Proposition 6.5. *If $M \models IE_1^- + \neg\sigma$ for some sentence $\sigma \in \forall E_1(\mathbb{N})$,* then $M_{\exp} \neq \mathbb{N}$.

Proof. If $M_i \neq M_{i+1}$ for each i then $M_{\exp} \neq \mathbb{N}$ by Proposition 6.3. Otherwise suppose $M_i \models E$ and $M \models \exists x\, \theta(x)$ with $\theta \in U_1$ and $\mathbb{N} \models \forall x \neg\theta(x)$. We shall show $M_i \models \exists x\, \theta(x)$ hence $M_i \neq \mathbb{N}$.

Let $\chi_i(x_0, x_1, \ldots, x_i)$ be $\chi(x_0, x_1) \wedge \chi(x_1, x_2) \wedge \cdots \wedge \chi(x_{i-1}, x_i)$ and consider the E_1 formula

$$\phi(y, a) \overset{\text{def}}{=} \theta(a) \to \exists x_1, \ldots, x_i \leq a\, \chi_i(y, x_1, \ldots, x_i).$$

If $a \in M$ satisfies $M \models \theta(a)$ then $a > \mathbb{N}$ and so $M \models \phi(0, a)$. Therefore

$$M \models \exists a\, (\phi(0, a) \wedge \neg\phi(a, a))$$

hence by JE_1 in M (Theorem 5.4)

$$M \models \exists a, x\, (\phi(x, a) \wedge \neg\phi(x + 1, a)),$$

but for such a, x we have $M \models \theta(a)$ and $x \in M_i$ so since $M_i \models E$ there are $x_1, x_2, \ldots, x_i \in M_i$ with

$$M \models \chi_i(x + 1, x_1, x_2, \ldots, x_i).$$

It follows that $x_i > a$ and so $a \in M_i$. Since θ is U_1, $M_i \models \theta(a)$ and we are done. □

Since $\forall E_1(\mathbb{N}) \vdash IE_1^-$ (in fact $\forall E_1(\mathbb{N}) \vdash I\forall E_1^-$, but I see no obvious way of using this 'extra' induction) we are left with the following question:

Problem 6.6. *Are there any nonstandard recursive models of* $\forall E_1(\mathbb{N})$?

This problem is related to the question of whether the E_n hierarchy collapses in $\mathbb{N}$, for if $E_1^{\mathbb{N}} = \Delta_0^{\mathbb{N}}$ then $\forall E_1(\mathbb{N})$ *and* $\Pi_1(\mathbb{N})$ would be equivalent, so the answer to 6.6 would be 'No'. In fact, assuming the existence of a nonstandard recursive model $M \models \forall E_1(\mathbb{N})$, our arguments give specific examples of Δ_0 formulas that are not equivalent (in $\mathbb{N}$) to any E_1 formula:

Proposition 6.7. *Suppose there is a surjection* $f : \mathbb{N} \to \mathbb{N}$ *with* E_1 *graph satisfying*

(i) $\forall x, y \in \mathbb{N}\,(f(x) < f(y) \to x < y)$,

(ii) *for some fixed* $k \in \mathbb{N}$

$$\forall x \in \mathbb{N}\, f^{(k)}(x) \leqslant \lfloor \log_2(x+1) \rfloor.$$

Then no countable nonstandard model $M \models \forall E_1(\mathbb{N})$ *is recursive.*

Proof (Sketch). Let $M \models \forall E_1(\mathbb{N})$ be nonstandard and note that $M \models \forall x\, \exists! y\, (f(x) = y)$. For each i let M_{i+1} be the initial segment of M defined by $\{f(x) \mid x \in M_i\}$, where $M_0 = M$. By (i) and '$f(x) = y$' being E_1 we have $M_i \neq \mathbb{N}$ for each i. If $M_0 = M_1 = M_2 = \cdots$ then $M \models I\Delta_0 + \exp$ since

$$M \models \forall x, z\, (f^{(l)}(x) > z \to \exists y < z\, \chi(x, y))$$

for some suitable $l \in \mathbb{N}$ by (ii). Otherwise $M_i \neq M_{i+1}$ for each i, and there are always cuts I closed under $+$, $\cdot$ such that $M_i \subseteq_e I \subseteq_e M_{i+1}$ for each i. By Matijasevič's Theorem, for all $\theta(z)$ in U_1 there is $m \in \mathbb{N}$ and polynomials p, q such that

$$\mathbb{N} \models \forall x\, \forall z < f^{(m)}(x)\, (\theta(z) \leftrightarrow \exists y \leqslant x\, p(x, y) = q(x, y)),$$

and this sentence is $\forall E_1$, so true in M. Hence for any finite fragment T of $\Pi_1(\mathbb{N})$ there is $i \in \mathbb{N}$ and $I \subseteq_e M$ with

$$M_i \subseteq_e I \models T.$$

So, just as in the proof of 6.3, we have $M_{\exp} = \bigcap_{i \in \mathbb{N}} M_i$ is a nonstandard initial segment of M satisfying $I\Delta_0 + \exp$. □

References

[1] P. Clote and G. Takeuti, Exponential time and bounded arithmetic, in: Structure of Complexity Classes, Lecture Notes in Computer Science 223 (Springer, Berlin, 1986) 125–143.

[2] C. Dimitracopoulos, Matijasevič's theorem and fragments of arithmetic. Ph.D. Thesis, Manchester University, 1980.

[3] H. Gaifman and C. Dimitracopoulos, Fragments of arithmetic and the MRDP theorem, Logic and Algorithmic, Monographie No. 30 de L'Enseignement Mathématique, 187–206.

[4] R. Kaye, J. Paris and C. Dimitracopoulos. On parameter free induction schemas, J. Symbolic Logic 53 (1988) 1082–1097.

[5] K. McAloon, On the complexity of models of arithmetic, J. Symbolic Logic 47 (1982) 403–415.
[6] J. Paris, O struktuře modelů omenzené E_1-indukce, Časopis pro pěstování Matematiky 109 (1984) 372–379.
[7] J. Paris and L. Kirby, Σ_n collection schemes in arithmetic, in: A. MacIntyre et al., eds., Logic Colloquium '77 (North-Holland, Amsterdam, 1978) 199–209.
[8] R. Parikh, Existence and feasibility in arithmetic, J. Symbolic Logic 36 (1971) 494–508.
[9] J. Robinson, Existential definability in arithmetic, Trans. Amer. Math. Soc. 72 (1952) 437–449.
[10] J. Shepherdson, Nonstandard models for fragments of number theory, in: J.W. Addison et al., eds., The Theory of Models (North-Holland, Amsterdam, 1965) 342–358.
[11] S. Tennenbaum, Non-archimedean models for arithmetic, Notices Amer. Math. Soc. 6 (1959) 270.
[12] G. Wilmers, Bounded existential induction, J. Symbolic Logic 50 (1985) 72–90.
[13] A. Wilkie, Some results and problems on weak systems of arithmetic, in: A. MacIntyre et al., eds., Logic Colloquium '77 (North-Holland, Amsterdam, 1978) 285–296.